2/2015

Datenschutz Nachrichten

38. Jahrgang
ISSN 0137-7767
12,00 Euro



■ Ein Ding, sie zu finden... ■ Grenzwertig… Drohnen im Migrationsregime ■ Grenzen sind nicht intelligent ■ Roboter auf Rädern ■ Schweigepflicht und IT-Dienstleistungen – ein Diskussionsbeitrag ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Samstag, 04. Juli 2015, 11:00 – 15:00 Uhr
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle.
dvd@datenschutzverein.de

Freitag, 09. Oktober 2015
DVD-Vorstandssitzung
Bonn. Anmeldung in der Geschäftsstelle.
dvd@datenschutzverein.de

Freitag, 09. Oktober 2015 – Samstag, 10. Oktober 2015
DVD-Jahrestagung in Bonn
Thema: Mobilität und Telematik (Arbeitstitel)

Sonntag, 11. Oktober 2015
DVD-Mitgliederversammlung in Bonn



Foto: Uwe Schlick / pixelio.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
38. Jahrgang, Heft 2

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Rheingasse 8-10, 53113 Bonn
Tel. 0228-222498
Konto 1900 2187, BLZ 370 501 98, Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Sönke Hilbrans
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Rheingasse 8-10, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@t-online.de

Druck
Onlineprinters GmbH
Rudolf-Diesel-Straße 10
91413 Neustadt a. d. Aisch
www.diedruckerei.de
Tel. +49 (0)91 61 / 6 20 98 00
Fax +49 (0) 91 61 / 66 29 20

Bezugspreis
Einzelheft 12 Euro. Jahresabonnement 42 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Das Jahresabonnement kann zum 31. Dezember eines Jahres mit einer Kündigungsfrist von sechs Wochen gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Frans Jozef Valenta, soweit nicht anders gekennzeichnet

Editorial

Liebe Leserin,
lieber Leser,

auf den ersten Blick liegt es nicht gerade nahe, die Bilder roher Gewalt in garnicht so fernen Ländern und die Eindrücke handfester Katastrophen und zahlreicher Opfer auf dem Mittelmeer mit Datenverarbeitung und Datenschutz in Beziehung zu setzen. Aber wir wurden schnell fündig: Schon das deutsche Asyl- und Ausländerrecht enthalten eine Vielzahl von Datenverarbeitungsregelungen, ohne die auch das Ausländerzentralregister (AZR) nicht betrieben werden dürfte. Auf Europäischer Ebene wird mit dem Schengener Informationssystem eine Verbunddatenbank betrieben, in der Einreiseverweigerungen europaweit ausgeschrieben werden können. Diese Instrumente reagieren nicht zuletzt auf die hohen Flüchtlingszahlen der späten 80er und der 90er Jahre. Auch mittels Datenerhebung und -verarbeitung konnte ein System errichtet werden, dass die gegenseitige Anerkennung von Visa und Aufenthaltstiteln in der EU ermöglichte und andererseits einheitliche Standards der Migrationskontrolle auch an den Außengrenzen enthalten soll. Für Deutschland hatte dies den erwünschten Nebeneffekt, dass es die meisten hier Schutz suchenden in andere Mitgliedstaaten zurückschicken durfte. Schon diese Möglichkeit stand freilich häufig nur auf dem Papier.

Heute ist Europa, nach einem Jahrzehnt relativ niedriger Flüchtlingszahlen, wieder Ziel von hunderttausenden von Schutzsuchenden. Für die Regierungen stellen sie die Grenzkontrolle und das System der Verteilung von Flüchtlingen in der Europäischen Union vor eine Zerreißprobe. Es wäre nicht die erste, auf welche die Staaten mit Datenerhebungen und Informationsverbünden reagieren würde.

Diese Ausgabe der DANA widmet sich dem Stand der informationstechnischen Lösungen auf dem Gebiet der Migrationskontrolle. Vieles wird Ihnen bekannt vorkommen: Weder raumgreifende Fingerabdruckerfassung und -verwendung, noch Aufklärungsdrohnen, noch das Versprechen „smarter“ Lösungen für alltägliche Kontrollaufgaben sind wirklich neu. Im Bereich der Migrationskontrolle spielen Resourcen häufig keine große Rolle; sie stellt nicht nur jede Politik (und jeden Politiker) der inneren Sicherheit auf die Probe, sondern dürfe sich auch als ideales Labor für technologische Großversuche erweisen. Der Blick an die Grenze könnte ein Blick in die Zukunft sein.

Eine instruktive Lektüre wünscht Ihnen

Sönke Hilbrans

Autorinnen und Autoren dieser Ausgabe:

Jochen Brandt
Dipl. Wirtschafts- und Arbeitsjurist (HWP), ist seit mehreren Jahren als externer Datenschutzbeauftragter, Trainer, Berater und Autor tätig. Außerdem ist er Geschäftsführer der Grid eG.
E-Mail: Info@Brandtschutz.de

Volker Eick
ist Politikwissenschaftler und arbeitet in Berlin. Email: eickv@zedat.fu-berlin.de

Dr. Andreas Höpken
langjährig als Datenschutzberater und externer Datenschutzbeauftragter tätig. Seine Schwerpunkte liegen dabei im medizinischen und sozialen Bereich. Er ist Vorstandsvorsitzender der Grid eG (www.Grideg.de und E-Mail: Hoepken@grideg.de).

Matthias Monroy
Wissensarbeiter, Aktivist und Mitglied der Redaktion der Zeitschrift „Bürgerrechte & Polizei/CILIP“. In Teilzeit Mitarbeiter des MdB Andrej Hunko. Publiziert in Zeitungen, Zeitschriften und Online-Medien, bei Telepolis, Netzpolitik und in Freien Radios. Alle Texte und Interviews unter digit.so36.net, auf Twitter@gipfelsoli

Eric Töpfer
arbeitet als Wissenschaftlicher Mitarbeiter am Deutschen Institut für Menschenrechte zu den Themen Innere Sicherheit und Datenschutz. Daneben ist er Redakteur der Zeitschrift „Bürgerrechte & Polizei/CILIP“. Der Beitrag gibt seine persönliche Meinung wieder. Kontakt: toepfer@emato.de

Eric Töpfer

Ein Ding, sie zu finden...

Eurodac und die biometrische Erfassung asylsuchender und irregulärer Migranten

2,4 Mio. erfasste Datensätze und täglich mehr als 1.300 Zugriffe – Eurodac ist das technische Rückgrat des Gemeinsamen Europäischen Asylsystems.[1] Errichtet durch die Verordnung (EG) Nr. 2725/2000 des Rates von Dezember 2000 und die ergänzende Durchführungsverordnung (EG) Nr. 407/2002 von Februar 2002 soll das System die „effektive Umsetzung" des Dublin-Regimes sicherstellen. Konzipiert ist Eurodac als zentrale daktyloskopische Datenbank, inklusive Automated Fingerprint Identification System (AFIS), mit Sitz in Straßburg und einem Backup-System im österreichischem Sankt Pongau, an die sternförmig sogenannte National Access Points – nationale Einwanderungs- oder Polizeibehörden in den Mitgliedstaaten – angeschlossen sind. Verwaltet wird das System seit 2012 von der neugeschaffenen EU-Agentur für das Betriebsmanagement der großen europäischen IT-Systeme (eu-LISA) im estnischen Tallinn. Inzwischen beteiligen sich 32 Länder – alle 28 EU-Mitglieder und die vier Schengen-Staaten Norwegen, Island, Schweiz und Liechtenstein. Damit ist Eurodac noch vor dem Schengen-Informationssystem das meistgenutzte der großen IT-Systeme im europäischen „Raum der Freiheit, der Sicherheit und des Rechts".

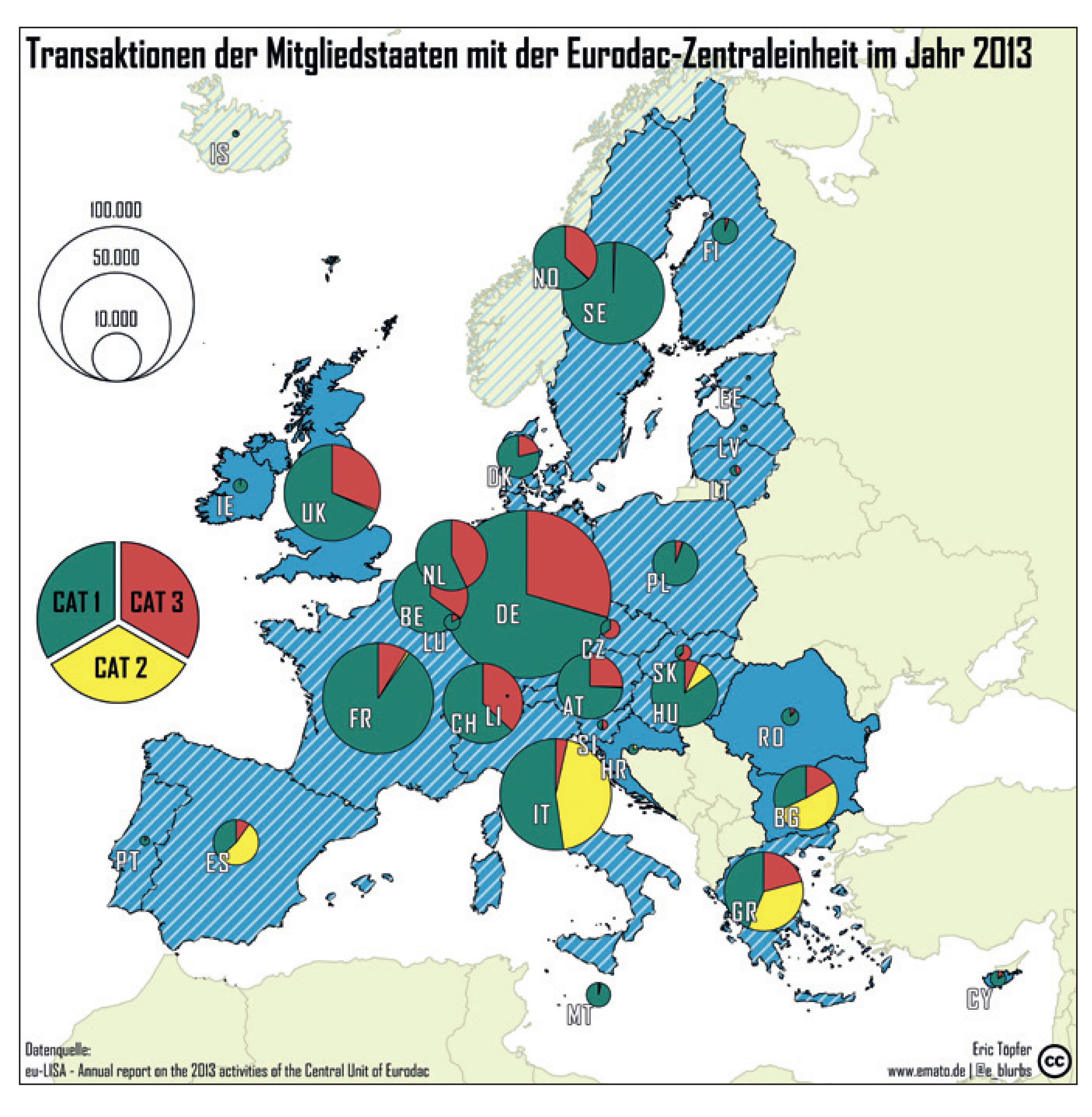
Verarbeitet werden i.d.R. die Abdrücke aller zehn Finger von Migranten aus drei Personenkategorien: Asylsuchende („Kategorie 1" – Speicherfrist 10 Jahre); Ausländer, die bei der irregulären Einreise an den Außengrenzen aufgegriffen werden („Kategorie 2" – Speicherfrist zwei Jahre); optional können die Teilnehmerstaaten zusätzlich die Fingerabdrücke von Irregulären erheben, die auf ihrem Territorium im Hinterland aufgegriffen werden („Kategorie 3" – keine Speicherung). Zusätzlich zu den Fingerabdrücken werden nur wenige Angaben zum Geschlecht, Ort und Zeitpunkt des Asylantrags bzw. Aufgriffs sowie der erkennungsdienstlichen Behandlung und Datenübermittlung und eine standardisierte Kennnummer gespeichert. Ein unmittelbarer biometrischer Abgleich mit dem Datenbankbestand findet durch die Eurodac-Zentraleinheit nur für Daten der Kategorie 1 und 3 statt, wobei letztere anschließend gelöscht werden müssen. Daten der Kategorie 2 werden bei der Anlieferung technisch getrennt von den Daten zu Asylsuchenden „nur" gespeichert und stehen somit für spätere Abgleiche zur Verfügung. Zweck der Datenverarbeitung ist es, zu erkennen, ob asylsuchende oder irreguläre Migranten bereits zuvor in einem anderen Teilnehmerstaat aktenkundig geworden sind. Verhindert werden sollen auf diese Weise das sogenannte „Asyl Shopping" und „sekundäre Migration", da im Rahmen des Dublin-Regimes jeweils nur ein Staat für die Bearbeitung von Anträgen auf internationalen Schutz zuständig ist – meist der Ankunftsstaat, d.h. i.d.R. ein Land an der südlichen oder östlichen Peripherie Europas.

Kafkaeske Verantwortlichkeiten

Auch wenn die National Access Points formal die nationalen Schnittstellen zur Eurodac-Zentraleinheit sind, sind die eigentlichen Datenlieferanten eine unübersichtlichen Anzahl von Behörden in den Mitgliedstaaten. Je nach Personenkategorie und Kontrollsituation sind dies in Deutschland z.B. die Außenstellen des Bundesamtes für Migration und Flüchtlinge (BAMF), Dienststellen der Bundespolizei sowie Ausländerbehörden oder Erkennungsdienste der Landespolizeien. Letztlich sind es diese Behörden, die für die Rechtmäßigkeit der Datenerhebung, -übermittlung, -speicherung und -abfragen sowie die Aktualität und Richtigkeit der Daten verantwortlich sind. Von ihnen hängt es z.B. ab, ob die Daten von Betroffenen tatsächlich bei der Zentraleinheit gelöscht werden, wenn sie eingebürgert werden. Ob und wie diese Stellen ihrer datenschutzrechtlichen Verantwortung gerecht werden, darüber ist wenig bekannt. Doch bereits die gemeinsame Aufsicht durch den Europäischen Datenschutzbeauftragten und seine Kollegen in den Mitgliedstaaten scheint sich äußerst schwierig zu gestalten. Im Bericht zur ersten koordinierten Überprüfung von 2007 liest man: „Eines der auffälligsten (und unerwarteten) Ergebnisse der Inspektion war, dass die Datenschutzbehörden in einigen Ländern sehr große Schwierigkeiten hatten, alle Behörden mit Eurodac-bezogenen Verantwortlichkeiten, geschweige denn die tatsächlich datenverarbeitende Stelle zu identifizieren. In einigen Fällen erheben die Polizeibehörden Daten, die Asylbehörden weiterverarbeiten (d.h. sie an die Zentraleinheit versenden und das Ergebnis des Vergleichs an die anfragende Behörde übermitteln). Zwar ist nicht zu beanstanden, wenn Zuständigkeiten geteilt werden, aber in manchen Mitgliedstaaten führte dies zu der Situation, dass keine der Behörden die Verantwortung für Probleme übernehmen wollte, die beim Betrieb von Eurodac aufkommen. Es scheint sogar, dass in zwei Mitgliedstaaten die Eurodac-Endnutzer weder voneinander wissen noch ihre exakte Rolle bei der Datenverarbeitung kennen."[2] Seitdem haben die Datenschutzbeauftragten das Thema nicht erneut aufgriffen. Doch selbst wenn sie sich im Labyrinth der Eurodac-Datenverarbeitung inzwischen zurecht gefunden haben, muss bezweifelt werden, dass dies Betroffenen gelingt, zumal, wenn sie in mehreren Ländern erfasst wurden.

Von menschlichen und technischen Fehlern

Dass die erkennungsdienstliche Behandlung und Archivführung in den hunderten von Dienststellen, in denen



europaweit Asylsuchende und Irreguläre erfasst werden, immer mit der Präzision eines Schweizer Uhrwerks abläuft, ist schwer vorstellbar. Menschliche Fehler wie die Verwechselung von Fingerabdruckblättern oder die Ergänzung falscher Angaben zur Person sind ebenso wenig auszuschließen wie Kommunikationsprobleme zwischen beteiligten Behörden. So ergab 2011 eine koordinierte Prüfung der Aufsichtsbehörden, dass in mindestens fünf Mitgliedstaaten Abstimmungsprobleme zwischen den Immigrationsbehörden und den National Access Points bestehen, die dazu führen, dass die vorgeschriebene vorzeitige Löschung der Eurodac-Einträge bei Einbürgerung nicht gewährleistet ist.[3] Selbst dort, wo die Prozesse inzwischen mittels Fingerabdruck-Livescannern, maschineller Benutzerführung und informationstechnischer Vernetzung weitgehend papierlos und automatisiert sind, schlummern Fehlerquellen. Etwa 20 Seiten lang sind z.B. die Kapitel der BAMF-Dienstanweisung zur erkennungsdienstlichen Behandlungen, und es finden sich Sätze wie dieser: „Liegt ein EURODAC-Treffer vor, ist es unbedingt erforderlich, die eMail, die über den EURODAC-Treffer informiert, in die MARiS-Schriftstückliste [MARiS ist das Workflow- und Dokumentenmanagementsystem des BAMF zur Vorgangsbearbeitung im Asyl- und Dublinverfahren] aufzunehmen. Aus technischen Gründen kann diese eMail derzeit nicht systemgesteuert in die MARiS-Schriftstückliste aufgenommen werden. Der Text der eMail ist deshalb in ein Word-Dokument zu kopieren, auf dem Desktop abzulegen und anschließend in die MARiS-Schriftstückliste auf-

zunehmen. Das aufgenommene Word-dokument wird in der Schriftstückliste zunächst mit der Bezeichnung ‚Import Word‘ angezeigt und muss deshalb mit dem Indizierbegriff ‚EURODAC-Treffer‘ umbenannt werden.“[4]

Spricht man mit Flüchtlingsberatungsstellen, werden vereinzelt Geschichten von Eurodac-Verwechslungen berichtet, die vermutlich ihren Ursprung in Fehlern bei der lokalen Registrierung haben. Ein systematischer Überblick über solche Fälle fehlt allerdings. Eine Idee von den Schwierigkeiten gibt jedoch der andauernde Streit um die Qualität der angelieferten Fingerabdruckdaten zwischen Eurodac-Zentraleinheit und den Mitgliedstaaten. 2013 wurden zehn Prozent der angelieferten Datensätze vom Eurodac-AFIS zurückgewiesen, weil sie dort für einen biometrischen Abgleich ungeeignet waren – aus einigen Ländern wurde und wird sogar jeder dritte Datensatz abgelehnt.[5] Zurückgeführt werden die Schwierigkeiten u.a. auf Probleme durch die manuelle Erfassung auf Fingerabdruckblättern, die in einigen EU-Ländern noch verbreitet scheint, und schlecht ausgebildetes, überfordertes oder unmotiviertes Personal. Dass solche Ursachen allein die Qualität der Fingerabdrücke beeinträchtigen, ist kaum wahrscheinlich.

Ein weiterer Grund für die hohen Ablehnungsraten ist die äußerst geringe Fehlertoleranz des AFIS der Eurodac-Zentraleinheit. Hintergrund hierfür ist, dass das eingesetzte Biometric Matching System der Firma 3MCogent anders als klassische kriminalpolizeiliche AFIS ein „Lights out“-System ist, d.h. es werden mutmaßlich eindeutige „Treffer“ ausgegeben, die ohne Verifizierung durch Daktyloskopie-Experten an die National Access Points weitergeleitet werden. Angeblich liegt die Wahrscheinlichkeit von falschen Treffern („false positives“) des Systems bei nahezu Null, doch gelegentlich werden Einzelfälle durch Meldungen aus den Mitgliedstaaten bekannt,[6] die für die endgültige Identifizierung verantwortlich sind. Wie der Identifizierungsprozess vor Ort organisiert ist, bleibt den Eurodac-Teilnehmern bislang jedoch selbst überlassen. Entsprechend unterschiedlich gestaltet sich die Praxis: Während in Deutschland das Bundeskriminalamt berichtet, dass im AFIS-Referat seiner Abteilung Zentrale Dienste jeder Eurodac-„Treffer“ durch zwei ausgebildeten Daktyloskopen nach Vier-Augen-Prinzip verifiziert wird, erfolgt die Überprüfung in Ländern wie Belgien, Finnland oder Slowenien mit Hilfe von nationalen AFIS vollautomatisiert – mit unbekannten Konsequenzen.[7]

Nicht geredet wird auch darüber, dass der Preis für die äußerst niedrige „false match rate“ – folgt man den Lehrbüchern der Biometrie – eine relativ hohe „false non-match rate“ sein muss, und entsprechend eine unbekannte Anzahl von bereits in Eurodac erfassten Asylsuchenden und Irregulären beim automatisierten Abgleich durch die Zentraleinheit als „false negatives“ unerkannt bleibt. Dass Betroffenen selbst hieraus problematische Folgen erwachsen können, illustriert der Fall von zwei somalischen Schwestern, die 2012/13 nach eigenen Angaben zusammen über Italien und Österreich nach Deutschland eingereist waren, dann aber auf unabsehbare Zeit getrennt wurden, als nur eine Schwester aufgrund eines Eurodac-„Treffers“ nach Italien zurückgeschoben wurde, die andere mangels „Treffers“ jedoch nach Österreich.[8]

Grundrechte unter Beweislast

Zur Überprüfung der in Eurodac über sie gespeicherten Daten und ihrer eventuellen Korrektur oder Löschung haben Betroffene theoretisch von jedem Mitgliedstaat aus das Recht auf Auskunft. Im Jahr 2013 gab es jedoch nur 49 solcher als „Kategorie 9“ bezeichneten Sonderanfragen an die Zentraleinheit – die meisten davon aus Frankreich, von wo berichtet wird, das Nichtregierungsorganisationen in der Region Calais Migranten zur Wahrnehmung ihrer Auskunftsrechte ermunterten.[9] Doch offensichtlich und wenig überraschend hat die Mehrheit der Menschen auf der Flucht ganz andere Sorgen. Hinzu kommt, dass die obligatorische Information über die in der Eurodac-Verordnung verbrieften Betroffenenrechte schwierig ist. Auch wenn schriftliche Informationen in verschiedenen Sprachen angeboten werden oder Dolmetscher Analphabeten mündlich informieren, so gehen im Asylverfahren die auf Eurodac bezogenen Hinweise häufig in der Masse der Informationen unter. Zudem gibt es Hinweise darauf, dass jenseits der Routinen des Asylverfahrens die entsprechenden Eurodac-Vorschriften nicht immer bekannt sind, so dass keineswegs sicher ist, dass Irreguläre während der erkennungsdienstlichen Behandlung regelmäßig über ihre Rechte aufgeklärt werden.[10]

Als Fußnote zu den eigentlich für Auskunftsersuchen reservierten „Kategorie 9“-Abfragen sei erwähnt, dass diese in den frühen Jahren von Eurodac in einigen Mitgliedstaaten massiv und rechtswidrig zu völlig anderen Zwecken missbraucht wurden, z.B. um verschlampte Treffermeldungen erneut abzufragen oder zu Test- und Trainingszwecken.[11] 2005 gab es mehr als 2.300 solcher Abfragen; allerdings ging der Missbrauch nach Intervention der EU-Kommission deutlich zurück, und der Verdacht, dass die Daten systematisch für polizeiliche Zwecke abgefragt worden waren, ließ sich nicht bestätigen.

Festzuhalten bleibt, dass jenseits der koordinierten „Inspektionen“ durch die Aufsichtsbehörden – tatsächlich häufig nur Email-Umfragen unter den an Eurodac beteiligten Behörden – wenig Informationen zu Problemen des Wirkbetriebs von Eurodac vorliegen. Betroffene selbst wagen fast nie, den vermeintlichen Wahrheitsgehalt eines Eurodac-„Treffers“ in Frage zu stellen. Entsprechend unangefochten konnten sich die Eurodac-„Treffer“ zum entscheidenden Faktor für die Zuständigkeitsbestimmung im Dublin-Verfahren entwickeln, obwohl de jure humanitäre Kriterien wie der Wunsch auf Familienzusammenführung Priorität haben müssten. Die häufig maßgeblich über Eurodac erhobenen Informationen zum Reiseweg ersetzen häufig weitere Befragungen, oder aber diese Befragungen finden erst statt, lange nachdem ein Dublin-Verfahren aufgrund eines Eurodac-„Treffers“ eingeleitet wurde – dann in der Regel zu spät.[12] In Deutschland z.B. wurden 2013 zwei Drittel der mehr als 35.000 Übernahmeersuchen, die an andere Mitgliedstaaten gerichtet wurden, aufgrund eines Eurodac-„Treffers“ gestellt.[13]

Widerstände …

Insbesondere auf Betreiben Deutschlands war die biometrische Erfassung

Irregulärer in der Eurodac-Verordnung festgeschrieben worden.[14] Damit war das System von Anfang an nicht nur als Instrument zur Umsetzung des Dublin-Regimes, sondern zur Migrationskontrolle per se angelegt. Zwar scheint Eurodac hinsichtlich der Detektion von mehrfach gestellten Asylanträgen seinen Zweck weitgehend zu erfüllen. Doch allen technokratischen Steuerungsvisionen zum Trotz scheitert die biometrische Totalerfassung irregulärer Migranten sowohl an nationalen Interessen als auch an Verzweiflung der Migranten selbst.

War die EU-Kommission bei der Ausschreibung der technischen Entwicklung Eurodacs noch davon ausgegangen, dass jährlich etwa 400.000 Datensätze der „Kategorie 2“ anfallen würden, so machte sich schnell Ernüchterung breit. Im ersten Jahr des Betriebes wurden nicht einmal 8.000 Datensätze aus den Mitgliedstaaten angeliefert.[15] Bis 2013 war die Zahl auf knapp 50.000 angestiegen – davon erwartungsgemäß die meisten aus den Grenzländern Italien, Griechenland und Bulgarien. Sah sich der EU-Ministerrat angesichts der Unterschiede zwischen Eurodac-Treffern und anderen Statistiken zur irregulären Einwanderung 2004 noch dazu veranlasst festzustellen, dass die Pflicht zur biometrischen Erfassung von beim irregulären Grenzübertritt aufgegriffenen Ausländern keineswegs auf das unmittelbare Grenzgebiet beziehe, vermeldete der Eurodac-Tätigkeitsbericht 2013 nur noch in nüchternem Bürokratensprech: „Die Diskrepanz zwischen der Statistik zu den in Eurodac gespeicherten „Kategorie 2“-Daten und anderen statistischen Quellen zum Umfang irregulärer Grenzübertritte in den Mitgliedstaaten ergibt sich aus der Interpretation von Artikel 8 (1) der aktuellen Eurodac-Verordnung.“ [16]

Doch selbst wenn die Grenzbehörden der südlichen und östlichen EU-Staaten „Kategorie 2“-Daten anliefern, geschieht dies teilweise mit solcher Verspätung, dass die aufgegriffenen Personen bis dahin längst weitergereist sein können, um nördlich der Alpen ihr Glück zu suchen. So vergingen z.B. in Griechenland im Jahr 2013 durchschnittlich 45 Tage zwischen der erkennungsdienstlichen Behandlung und dem Übersenden der Daten an die Eurodac-Zentraleinheit. [17] Auf diese Weise unterlaufen die Länder an der südlichen und östlichen Peripherie – sei es kalkuliert oder schlicht, weil die Behörden überfordert sind – die Logik Eurodacs – sehr zum Ärger der Regierungen in jenen Ländern, die das eigentliche Ziel der Migranten sind.

Doch auch die Migranten selbst wissen inzwischen um die Bedeutung ihrer Fingerabdrücke. Und so nehmen Berichte zu über mutmaßliche Selbstverstümmelungen der Fingerkuppen durch Verbrennung, Verätzung und Verletzungen durch Messer oder Schleifpapier, die eine biometrischen Abgleich mit Eurodac unmöglich machen. Dabei ist allerdings keineswegs immer klar, ob die „Nicht-Lesbarkeit“ der Fingerabdrücke wirklich absichtlich selbst herbeigeführt wurde oder nicht andere Ursachen hat und z.B. altersbedingt oder auf schwere Handarbeit zurückzuführen ist.

… und Zwang

Und so stehen die teilnehmenden Behörden vor der Frage, wie sie mit jenen Menschen umgehen, die sich nicht in das System einlesen lassen. In Deutschland schreiben § 15 des Asylverfahrensgesetzes und § 49 des Aufenthaltsgesetzes vor, dass Ausländer zur Aufklärung des Sachverhaltes im Asylverfahren bzw. bei Zweifeln an ihrer Identität verpflichtet sind, erkennungsdienstliche Maßnahmen „zu dulden“. Tun sie dies nicht, können Zwangsmaßnahmen angeordnet werden. Die Bundesregierung berichtet, dass dies „aufgrund der Kooperationsbereitschaft der Drittausländer in der Regel allerdings nicht notwendig“ sei.[18] Bei Asylsuchenden ist dies auch wenig überraschend – droht ihnen doch bei mangelnder Mitwirkung an der biometrischen Erfassung die Einstellung des Asylverfahrens und damit die Abschiebung.[19] Doch insbesondere bei Irregulären geht die für sich genommen bereits entwürdigende erkennungsdienstliche Behandlung in der Praxis durchaus mit recht deutlichen Eingriffen einher: So wurde aus Berlin bekannt, dass unbegleitete Minderjährige, die des irregulären Aufenthalts verdächtigt werden, zur Abnahme ihrer Fingerabdrücke für bis zu sechs Stunden in polizeilichen Gewahrsam genommen und dort regelmäßig zur „Vermeidung einer Fremd- oder Eigengefährdung“ Leibesvisitationen unterzogen werden.[20]

Aus anderen EU-Staaten wird berichtet, dass Asylsuchende, denen unterstellt wird, das Eurodac-„Enrolment“ durch eine absichtliche Manipulation ihrer Fingerkuppen zu unterlaufen, gleich für mehrere Wochen inhaftiert werden, bis die Prozedur wiederholt werden kann, oder ihnen zur Strafe Leistungen gekürzt werden.[21] Bislang scheint nur eine Minderheit von Eurodac-Teilnehmerstaaten zu solch rabiaten Methoden zu greifen. Doch in den EU-Institutionen denkt man inzwischen hinter vorgehaltener Hand über die Harmonisierung solcher Praktiken nach.[22] Was allerdings mit Menschen geschieht, bei denen es tatsächlich und ohne ihr Zutun unmöglich ist, ihnen Fingerabdrücke abzunehmen, darauf bleibt die Europäische Union bis heute eine Antwort schuldig. Denn anders als z.B. der Visa-Kodex für die biometrische Erfassung von Visumsantragstellern sieht die Eurodac-Verordnung keine Ausnahmen vor – auch nicht in ihrer Neufassung, die am 20. Juli 2015 in Kraft treten wird.

Alles neu? Die Polizei greift nach Eurodac

Der Verabschiedung der neuen Eurodac-Verordnung (EU) Nr. 603/2013 war ein langjähriges politisches Tauziehen um die Öffnung der Fingerabdruck-Datenbank für den Zugriff der Polizei- und Strafverfolgungsbehörden vorausgegangen. Seit 2001 hatte u.a. die deutsche Regierung im Ministerrat auf die Ausweitung der Nutzungsmöglichkeiten gedrängt.

Einen ersten Vorschlag für eine neue Eurodac-Verordnung hatte die EU-Kommission bereits im Dezember 2008 vorgelegt. Dieser zielte auf eine „verbesserte Funktionsweise“ und wollte insbesondere das Unterlaufen des Dublin-Regimes durch die Grenzländer verhindern, indem er festgelegte Fristen zur Übermittlung der Daten an die Zentraleinheit vorschrieb sowie einige Datenschutzprobleme auszubessern suchte, die durch die koordinierten Prüfungen der Aufsichtsbehörden deutlich geworden waren. Außerdem sollte die Durchführungsverordnung integriert werden und die Verwaltung Eurodacs durch die

EU-Agentur eu-LISA geregelt werden.

Im September 2009 gab die Kommission schließlich dem Druck aus dem Ministerrat nach und legte auch einen Entwurf für einen Ratsbeschluss vor, der Eurodac für den Zugriff der Sicherheitsbehörden öffnen sollte. Obwohl die Kommission nach Inkrafttreten des Lissabon-Vertrages und der Vergemeinschaftung der Polizei- und Justizkooperation noch einmal den Versuch unternahm, das Thema auszuklammern, um zu einer schnellen Lösung im Rahmen des Asylpaketes zu kommen, scheiterte sie am Veto des Rates. Es vergingen weitere anderthalb Jahre, bis die Kommission 2012 schließlich beide Vorschläge, die auf dem Tisch lagen, zusammenfasste. Trotz erheblicher Kritik im Europäischen Parlament, durch Datenschützer und Zivilgesellschaft, dass durch den polizeilichen Zugriff auf Eurodac eine zusätzliche Stigmatisierung der vulnerablen Flüchtlinge droht, wurde die Neuverordnung am 26. Juni 2013 im Rahmen des EU-Asylpaketes verabschiedet, inklusive der Regelungen zu „Anträgen der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten".

Verbindlich wird damit ab Sommer 2015 eine 72-Stunden-Frist binnen derer die Mitgliedstaaten Fingerabdruckdaten an die Eurodac-Zentraleinheit zu übermitteln haben – bislang war lediglich vage von „unverzüglich" die Rede. Gestärkt werden soll die Verfahrenssicherheit zur eindeutigen Identifizierung, indem künftig in allen Mitgliedstaaten die „Treffer"-Meldungen der Zentraleinheit von Daktyloskopie-Experten verifiziert werden müssen. Die Informationsrechte der Betroffenen werden durch neue Vorgaben zur verständlichen Belehrung gestärkt. Verkürzt wird die Speicherfrist für Daten der „Kategorie 2" von 24 auf 18 Monaten. Eine deutliche Verschlechterung stellt allerdings die Entscheidung dar, dass die Fingerabdruckdaten von Asylsuchenden in der „Kategorie 1" nicht länger sofort für den Zugriff gesperrt werden, wenn sie als Flüchtlinge anerkannt werden. Kosmetisch markiert, bleiben sie noch weitere drei Jahre für den biometrischen Vergleich abrufbar. Somit bleibt der Generalverdacht selbst dann, wenn internationaler Schutz gewährt wird.

Durchgesetzt haben sich bei letzterem Punkt vermutlich die Interessen der Sicherheitsbürokratien. Andererseits aber hat das Europaparlament versucht, die die Hürden für den polizeilichen Zugriff hoch zu legen: Für einen Abgleich von Fingerabdrücken mit Eurodac muss nachgewiesen werden, dass zuvor vergeblich nationale Datenbanken, der Prüm-Verbund und das Visa-Informationssystem abgefragt wurden. Zu beschränken ist der Abgleich auf Zwecke der „Verhütung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten", und systematische Massenabfragen sind untersagt. Allerdings hat man den Bock zum Gärtner gemacht, denn als nationale „Prüfstellen", ob all diese Bedingungen vorliegen, sind Sicherheitsbehörden zu benennen. Wir dürfen also gespannt sein, was das neue Kapitel in der Geschichte Eurodacs bringt.

1 Zahlen für 2013 aus: eu-LISA (2014): Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000. Tallinn, S. 20ff.

2 Eurodac Supervision Coordination Group (2007): Report of the first coordinated inspection. Brüssel, S. 13. Übersetzung des Autors.

3 Eurodac Supervision Coordination Group (2011): Coordinated inspection report on advance deletion of data. Brüssel, S. 5.

4 Bundesamt für Migration und Flüchtlinge (2014): Dienstanweisung AVS. Kapitel „Ed-Behandlung mittels Livescan", S. 2.

5 eu-LISA (2014): Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000, S. 18.

6 2007 wurde erstmals ein „false positive" berichtet. Vgl. Tätigkeitsbericht 2008 der Eurodac Zentraleinheit. KOM(2009) 494 endg. v. 25.9.2009, S. 3

7 European Migration Network (2011): Ad-Hoc Query on the implementation of Council regulation 2725/2000 (Eurodac), Brüssel.

8 Der Fall wurde vor dem VG Ansbach verhandelt. S. Beschluss vom 18.09.2013, Az. AN 2 K 13.30675.

9 eu-LISA (2014): Annual report in the 2013 activities of the Central Unit of Eurodac, S. 12.

10 Vgl. z.B. Bender, Dominik; Bethke, Maria (2012): Zehn Jahre Dublin - kein Grund zum Feiern. Zur Umsetzung der Dublin-II-Verordnung in Deutschland. Hessischer Flüchtlingsrat. Frankfurt am Main, S. 14.

11 Eurodac Supervision Coordination Group (2007): Report of the first coordinated inspection, S. 9.

12 Vgl. Bender, Dominik; Bethke, Maria (2012): Zehn Jahre Dublin - kein Grund zum Feiern. Zur Umsetzung der Dublin-II-Verordnung in Deutschland. Hessischer Flüchtlingsrat. Frankfurt am Main, S. 16ff.

13 Bundesministerium des Innern (Hg.) (2015): Migrationsbericht 2013. Berlin, S. 83.

14 Zur Genese der Eurodac-Verordnung vgl. Aus, Jonathan P. (2006): Eurodac. A solution looking for a problem? Centre for European Studies. Oslo (ARENA Working Paper, 9).

15 EG-Kommission (2004): First annual report to the Council and the European Parliament on the activities of the EURODAC Central Unit. SEC(2004) 557, 05.05.2004, S. 10.

16 eu-LISA (2015): eu-LISA (2014): Annual report on the 2013 activities of the Central Unit of Eurodac pursuant to Article 24(1) of Regulation (EC) No 2725/2000, S. 15. Übersetzung des Autors.

17 Ebda., S. 18.

18 Deutscher Bundestag (2014): Anwendung von Zwangsmaßnahmen gegenüber Schutzsuchenden zur Abgabe ihres Fingerabdrucks. Schriftliche Frage der MdB Luise Amtsberg (B90/Grüne) / Schriftliche Antwort des Parl. StS Ole Schröder. Drucksache 18/3476, 05.12.2014, S. 24f.

19 Vgl. BVerwG, Urteil vom 05.09.2013, Az. BVerwG 10 C 1.13.

20 Abgeordnetenhaus Berlin (2013): Erkennungsdienstliche Behandlung von unbegleiteten minderjährigen Flüchtlingen in Berlin II – bei der Polizei. Kleine Anfrage der Abgeordneten Katrin Möller und Hakan Taş (LINKE) vom 29. April 2013 (Eingang beim Abgeordnetenhaus am 29. April 2013) und Antwort. Drucksache 17/11992, 11.06.2013.

21 Eurodac Supervision Coordination Group (2013): Report on the coordinated inspection on unreadable fingerprints. Brussels.

22 Statewatch (2015): Fingerprinting by force. Secret discussions on „systematic identification" of migrants and asylum seekers. Online verfügbar unter http://www.statewatch.org/news/2015/feb/forced-fingerprinting.htm.

Volker Eick

Grenzwertig… Drohnen im Migrationsregime

Zwischen Ertrinken und Verdursten ist viel Platz. Der nachfolgende Beitrag situiert aktuelle Aufklärungskapazitäten von unbemannten technischen fliegenden Systemen,[1] für die sich der Begriff „Drohne" etabliert hat, mit Blick auf Grenzen. Der mexikanische und der Mittelmeer-Grenzraum dienen zur Illustrierung. Das Argument ist, Drohnen lösen in Grenzregimen zur Migrationsabwehr kein Problem, stellen aber einen lukrativen Markt dar.



MQ-1 Predator. Bild: Frans Valenta – Creative Commons CC BY-ND 3.0 DE

Drohnen, genauer Flugdrohnen, gibt es von der Größe eines Insektes, wie sie in Afghanistan bei der Aufklärung in Straßenzügen oder Gebäuden durch das britische Militär zum Einsatz kamen,[2] bis zu der eines Verkehrsflugzeuges, wie etwa die von Facebook und Google geplanten Solardrohnen über Afrika und Asien.[3]

Zahlen zählen

Neu sind Forschung an und Einsatz von (militärischen) Drohnen nicht – sie reichen bis in den Ersten Weltkrieg zurück.[4] Angesichts schrumpfender Militärhaushalte und wegen angenommener Kostenvorteile gegenüber anderem Fluggerät gelten sie heute als Wachstumsmarkt. Für Flugdrohnen mit größerer Reichweite (über 125 km) gehen jüngere Marktstudien, je nach Berechnungsgrundlage, für 2014 von einem Jahresumsatz zwischen 2,9 Mrd. und 11 Mrd. US-Dollar aus, der in 2020 auf 3,9 Mrd. bzw. 16 Mrd. US-Dollar steigen soll. Der Umsatzanteil von Militärdrohnen sinkt nach diesen Prognosen, liegt aber auch 2020 noch bei etwa 85 Prozent; pro Jahr würden demnach zwischen 1.000 und 2.500 Flugdrohnen produziert.[5]

Nach Umsatzzahlen dominieren die USA den Weltmarkt (35%), gefolgt von Israel (4,2%) und Europa (3,4%). Führend sind die US-amerikanischen Unternehmen Northrop Grumman (u.a. Global Hawk, EuroHawk), General Atomics Aeronautical Systems (u.a. Predator B/Reaper), AAI (u.a. Shadow), die staatliche Israel Aerospace Industries (u.a. Heron, Hunter) sowie das israelische Privatunternehmen Elbit Systems Ltd. (u.a. Hermes, Silver Arrow). In Europa hat im Februar 2015 ein Konsortium aus Frankreich (Dassault Aviation), Italien (Alenia), Schweden (Saab), Spanien (EADS CASA), der Schweiz (RUAG) und Griechenland (Hellenic Aerospace Industry) die zweite Testphase für die bewaffnete Tarnkappen-Drohne „nEUROn" abgeschlossen.[6] In Deutschland sind u.a. Diehl BGT Defence und Rheinmetall für die Bundeswehr aktiv.[7]

Auf den ersten Blick ist der (militärische) Drohnenmarkt big business für große staatliche und private Konzerne: Tatsächlich aber sind an jedem einzelnen „System" zahlreiche Firmen beteiligt und in komplexe Wertschöpfungsketten eingebunden, darunter, wie beim EuroHawk, auch kleine und mittelständische deutsche Unternehmen wie etwa die Information System Solutions AG aus Ravensburg, die u.a. Sensoren für Drohnen fertigt.[8]

Insgesamt produzieren 50 Länder Drohnen – darunter 16 auch bewaffnete Systeme[9] –, rund 80 haben sich Drohnen beschafft;[10] auch die UN und nichtstaatliche Akteure wie die Hisbollah besitzen Drohnen.[11] Nach einer jüngeren Studie des Stockholm International Peace Research Institute[12] sind zwischen 2010 und 2014 international 439 Flugdrohnen an 35 Länder exportiert worden, davon elf bewaffnete Systeme.[13] Israel exportierte 164 Flugdrohnen, die USA 132, Italien 37, Hauptabnehmer war Großbritannien mit 55 Systemen.

Der dumme Drohn?

Was der jeweilige Flugdrohn[14] – neben der Fähigkeit zur Langzeitüberwachung – „kann", hängt von der Ausstattung mit sogenannten Subsystemen ab. Neben der Bestückung mit (mehr oder weniger tödlichen) Waffen können dazu Kame-

ras zur Echtzeit-Videoüberwachung (ggf. mit Fähigkeiten zur Erkennung von Autokennzeichen, Gesichtern),[15] Wärmebildaufklärung,[16] Infrarotsensoren, Ortsbestimmungen (GPS, Galileo), Funkzellenabfragefähigkeiten (Abhören von Gesprächen, Mitlesen von SMS), Sensoren zur akustischen Überwachung, Messinstrumente zur Luftzusammensetzung (Gase, Gifte, Feuchtigkeit) und Radarsysteme (Abtastung der Erdoberfläche mit elektromagnetischen Wellen) gehören, die tags und bei Nacht, über Wolken oder in Sandstürmen „sehen" können.[17]

Als Faustregel darf gelten: je elaborierter das jeweils installierte Gerät, aber auch die Drohnen selbst, desto genauer (und störanfälliger) das System. Für die US-Luftwaffe wird davon ausgegangen, sie habe etwa ein Drittel ihrer Drohnen durch Un- und Ausfälle in Afghanistan, Pakistan und im Irak verloren,[18] bei der Bundeswehr beliefen sich die Verluste mit Stand 2014 auf bis zu zwei Drittel, etwa bei den Systemen LUNA und Heron I.[19] Da ihnen aber zahlreiche Kapazitäten zugesprochen werden, die sich mit herkömmlichem Fluggerät nicht erreichen ließen und ihr Einsatz für targeted killings und signature strikes als Erfolg betrachtet wird, werden Forschung und Produktion fortgesetzt und intensiviert. Während in den USA vor allem das Militär, seine Forschungseinrichtungen und das Department of Homeland Security Auftraggeber der untereinander konkurrierenden Rüstungskonzerne sind, fehlt es den europäischen Militärs bisher an einer gemeinsamen Strategie. Rüstungsfirmen, auf der Suche nach neuen Märkten, bedienen sich daher nicht nur diverser Lobbyorganisationen,[20] sondern zielen auch auf Fördergelder, die die EU-Kommission vor allem an Rüstungsfirmen als führende „Projektpartner" ausreicht.

Bereits 2006 bezeichnet die EU-Kommission das „Verfolgen und Überwachen von (nicht kooperativen) Personen, von Fahrzeugen und Substanzen als ausschlaggebende Fähigkeit", die als „automatisierte Überwachung und Kontrolle durch genaue und zuverlässige Raumbilder" erreicht werden müsse.[21] Auch in den Vorläufern der EU-Sicherheitsforschungsprogramme (FP), die z.T. mit nationalen Programmen unterlegt sind,[22] und verstärkt ab 2007 (FP 7) haben Drohnenprojekte eine prominente Rolle. Bis 2014 wurden mehr als 90 Forschungsprojekte zu Drohnen mit einem Budget von rund 315 Millionen Euro finanziert.[23]

Generell haben sich Grenzsicherung und Migrationsmanagement zu einem eigenständigen Experimentierfeld für Drohnen entwickelt. Dort soll aus Sicht der EU-Kommission demonstriert werden, dass Europa den Kampf um die Technologieführerschaft gewinnen will und kann, auch wenn gegenwärtig „die USA und Israel den Sektor dominieren. Die europäische Luftfahrtindustrie liegt weiterhin zurück und muss schnell den Anschluss finden, um auf diesem sich global entwickelnden Markt konkurrenzfähig zu sein".[24] Die US-amerikanischen Erfahrungen an der Grenze zu Mexiko, bei denen jeweils Drohnensysteme eine tragende Rolle spielen (sollen), gelten dabei als beispielgebend.[25]

Demarkationsdrohnen

Im Rahmen dieses Überwachungs- und Pazifizierungsregimes,[26] in dem Drohnen eine wichtige Rolle zugeschrieben wird, kommt es zu einer dreifachen, wenn auch widersprüchlichen Bewegung: Die Grenze als Demarkationslinie oder Checkpoint wird zu einem Grenzraum umdefiniert, aus dem Scheitern eines ursprünglich nach Außen gerichteten staatlichen Grenzschutzes wird die Notwendigkeit einer neuen Innenpolitik unter Beteiligung von kommerziellen[27] und „zivilgesellschaftlichen"[28] Akteuren abgeleitet. Im Rahmen der Technisierung des Migrationsmanagements wird drittens eine Militarisierung von Innenpolitik betrieben, in der unterschiedliche Kapitalfraktionen um Marktanteile konkurrieren.

Exemplarisch lässt sich das an der rund 3.100 Kilometer langen Grenze zwischen den USA und Mexiko zeigen, bei der insbesondere die 600 Kilometer zwischen Arizona und Mexiko zum Experimentierfeld für neuartige Formen der Demarkation geworden sind.[29]

Operation Arizona

Seit 1924 gibt es eine US-Grenzpolizei, für die bis in die 1940er Jahre die Grenze zwischen den USA und Mexiko faktisch keine Rolle spielte.[30] Billige und rechtlose Arbeitskräfte, die insbesondere zur Erntezeit auf die Obstplantagen in Kalifornien ein- und dann zurückwanderten, waren die Regel; im Norden waren Industriearbeiter gefragt. Die Grenzpolizei bestand damals aus rund 1.100 Bediensteten,[31] die sich reaktiv auf größere Städte und Grenzübergänge konzentrierten. Erst unter dem Eindruck der Wirtschaftskrise Mexikos Anfang der 1990er Jahre und im Vorfeld der Vereinbarung des Freihandelsabkommens NAFTA (1994) unter Präsident Clinton entwickelt sich eine gegen illegalisierte Grenzübertritte gerichtete sicherheitspolitische Debatte.[32] Sie führte zur Verschärfung des Einwanderungsgesetzes (1996) und massenhaften Abschiebungen, zum massiven Ausbau des Grenzschutzes sowie zur Stationierung von Militär und Nationalgarde entlang der Grenze. Erklärtes Ziel ist seitdem „Prävention durch Abschreckung".[33]

Der technologische Teil dieser Hochrüstung beginnt 1993 mit dem Projekt Blockade (später umbenannt in Hold the Line), das Stützpunkte für Grenzbeamte auf Überwachungstürmen mit Flutlichtanlagen, Bewegungssensoren, erstmals Hubschrauber und eine Schnelle Eingreiftruppe mit sich bringt.[34] Nachfolgeprojekte entstehen in Kalifornien (Operation Gatekeeper, 1994), Arizona (Operation Safeguard, 1994) und Texas (Operation Rio Grande, 1997), die unter Bundesaufsicht ausgebaut, einander angeglichen und über die Jahre fortgesetzt werden, aber in ihrer technologischen Ausrichtung auch in Konkurrenz zueinander stehen.[35]

1998 installieren die USA das Integrated Surveillance Intelligence System. ISIS verbindet Videofernüberwachung hochauflösender Kameras mit über- und unterirdischer Sensorentechnik (zur seismischen, magnetischen und thermischen Detektion) über Radio- und magnetische Wellen zu einem einheitlichen Computersystem, das die Informationen automatisch an die Grenzbehörden weiterleitet.[36] Das Projekt wird 2005 nach einer Reihe von Betrugs- und Korruptionsskandalen, Kosten von 239 Mill. US-Dollar und mehr als 90 Prozent Fehlermeldungen eingestellt.[37] Ein Jahr später wird es durch das US-Heimat-

schutz-Programm SBInet (Secure Border Initiative net) ersetzt, an dem Boeing Industries mit Project 28 beteiligt ist. Angekündigt als system of systems, werden auf einer Länge von 28 Meilen (45 km) neun Antennen mit Tageslicht-, Nachtsicht- und Infrarotkameras, mit Bewegungssensoren, Überwachungstürmen, sämtlichen Polizeifahrzeugen und einer Einsatzzentrale zu einem „virtual fence“ verbunden, der jedwede Veränderung erkennen, identifizieren, mittels Künstlicher Intelligenz auswerten, das Risiko einschätzen und entsprechende Gegenmaßnahmen einleiten soll.[38] Als die damalige Heimatschutzministerin Napolitano 2011 auch dieses Programm weitgehend einstellt,[39] weil es den Erwartungen nicht gerecht wird, sind nicht nur 1 Mrd. US-Dollar verbrannt, sondern es schlägt auch (wieder) die Stunde der Drohne.[40]

Flugdrohnen waren weder Teil von ISIS noch von SBI – der anhaltende Konkurrenzkampf zwischen den einzelnen Grenzschutzabteilungen und der Homeland Security mit ihren jeweiligen Industriepartnern gilt dafür als verantwortlich[41] – wurden aber ab 2003, basierend auf den Erfahrungen im Kosovo und in Afghanistan, von Militär und Heimatschutz parallel getestet. Sie werden zum Mittel der Wahl für das neue Programm, das auf mobile Überwachung, unbemannte Flugsysteme sowie Wärmebilderfassung setzt und für eine „effective balance between costs and capabilities“ sorgen soll.[42] Die Kampfdrohne mutiert zur Grenzdrohne. Der Regeleinsatz zur Grenzsicherung beginnt mit zunächst drei Drohnen des Typs Hermes 450 (Elbit Systems, Juni 2004), Hunter (Northrop Grumman, Januar 2005) und Predator B (General Atomics, August 2005).[43] Die jetzt 10.500 Grenzpolizisten an der südlichen Grenze mit ihren Stahlbarrieren, Überwachungstürmen, Fahr- und Flugzeugen, Helikoptern, Videokameras und Bodensensoren bekommen vernetzte Unterstützung.[44] Der Bestand an Drohnen wird auf sechs Exemplare aufgestockt, die jetzt auch den mexikanischen Grenzraum überwachen.[45] Die Arizona Border Control Initiative (2004) wird in den Arizona Border Surveillance Technology Plan (2011) umbenannt. Er umfasst die Installation von Wärmesensoren, von 38 mobilen Videoüberwachungseinheiten (Mobile Surveillance Systems) und intensiviert den Bau der derzeit 250 Überwachungstürme (Remote Video Surveillance Systems) entlang der Grenze; der Kontrakt wird an Elbit Systems vergeben.[46] Die jetzt acht Drohnen am mexikanischen Grenzraum stammen von General Atomics,[47] sind aber mit dem Arizona Plan ebensowenig verbunden wie ein weiteres Drohnenprojekt: BAE Systems erhält nach Tests im Jahr 2009 den Auftrag, zwei Drohnen – eine für Afghanistan, die andere für die mexikanische Grenze – mit dem militärischen System VADER (Vehicle and Dismount Exploitation Radar) auszurüsten; beide sind seit 2012 im Einsatz. VADER kann, anders als herkömmliche Radarüberwachung, langsamere und kleinere „Ziele“ erfassen, Bewegungen von Menschen und Tieren unterscheiden und aus 7,5 Kilometer Höhe auch durch Wolken und Sandstürme erkennen, mit Sensoren verfolgen und an Bodenstationen melden.[48] Allein zwischen Oktober und Dezember 2012 wurden so in Arizona über 7.300 illegalisierte Grenzübergänge gemeldet. Im Rio Grande Valley (Texas) – einer der kürzesten Sektoren, in den die Grenze eingeteilt ist – wurden 2012 fast 98.000 Personen beim versuchten Grenzübertritt festgenommen, eine Zunahme um 65 Prozent gegenüber dem Vorjahr.[49]

Im Jahr 2014 ist die Grenzpolizei auf fast 21.000 Kräfte angewachsen und am Boden im Besitz von automatisierten über- und unterirdischen Kameras und Sensoren, Nachtsicht- und Wärmebild- und Infrarotsystemen (FLIR-Radar), GPS-Anbindung, mobilen Röntgen- und Radioisotopgeräten (Fingerabdruck- und Substanzanalyse). In der Luft sind neben 250 Flugzeugen und Helikoptern auch Aerostat (ein mit Radar ausgestatteter Heliumballon, der über 320 Meter weit „sehen“ und Bodenaktivitäten wahrnehmen kann) und neun Drohnen,[50] von denen zwei mit VADER, weitere mit Synthetic Aperture Radar (SAR) ausgestattet sind.[51] Das Drohnenprogramm kostete zwischen 2005 und 2012 rund 360 Mill. US-Dollar, die Anschaffung von 14 weiteren Drohnen (802 Mill. USD) ist vorgesehen, aber umstritten, weil angekündigte Ergebnisse nicht erreicht wurden.[52]

Der unter Präsident Nixon begonnene War on Drugs wird in einen Krieg gegen Migration transformiert[53] und zeitigt dabei eine Reihe höchst disparater Ergebnisse, zu denen der Tod durch Verdursten im Grenzgebiet gehört.[54] Flüchtlinge und Arbeitsmigranten sind durch die blockierten üblichen und weniger gefährlichen Grenzübergangsrouten in die dirty, dangerous and deathly Regionen verwiesen, benötigen daher professionelle (und teure) Fluchthelfer. Arbeitsmigranten, denen dennoch der Grenzübertritt gelingt, gehen angesichts der Kontrollintensität nicht mehr zurück nach Mexiko, sondern bleiben in den USA.[55]

2005 wurden mehr als 1,2 Millionen illegalisierte Migranten von den Grenzschutzbehörden festgenommen, 2014 rund 480.000, darunter rund 36.000 unbegleitete Kinder. In sozialwissenschaftlichen Schätzungen wird davon ausgegangen, dass etwa jeder vierte Grenzübertritt verhindert werden kann, die Grenzschutzbehörden gehen von jedem fünften aus.[56] Eine Reaktion darauf ist der anhaltende Ausbau des Überwachungsapparats:

So sieht der vom US-Senat unter Präsident Obama verabschiedete, vom Repräsentantenhaus derzeit aber blockierte Border Security, Economic Opportunity and Immigration Modernization Act u.a. vor, dass bis 2017 der bisher 1.050 Kilometer lange Grenzzaun um weitere 1,126 Kilometer verlängert wird. 3.500 neue Grenzschützer sollen eingestellt sowie weitere Drohnen beschafft werden,[57] für die, wie 2013 bekannt wird, das Heimatschutzministerium seit 2010 die Bewaffnung mit less-lethal weapons, also weniger tödlichen Waffen, in Erwägung zieht.[58]

Eine weitere Reaktion ist das Zusammenschalten von Grenzdrohnen mit satellitengenerierten Georaumdaten, die im Processing Exploitation and Dissemination Center der Homeland Security zusammenlaufen. Am Boden eigenständig von den Drohnen entdeckte Anomalien sollen analysiert und so unentdeckte Korridore des Grenzübertritts erkannt werden. Dafür pendeln die Drohnen über drei Tage in der Luft und kehren entlang vordefinierter Routen zu ihrem Ausgangspunkt zurück. Zwischen März und Oktober 2013 fanden 10.000 solcher „Change Detection“-Flüge statt.

Erst wenn Auffälligkeiten gemeldet werden – die Fehlerquote liegt angeblich nur bei 4 Prozent –, greifen Grenzschutzkräfte ein.[59]

Eine dritte Reaktion definiert die südwestliche Grenzlinie als Südwestgrenzregion, als das Gebiet, „das in einem 100 Meilenabstand zur südlichen Grenze liegt“[60] und in dem Bürgerrechte suspendiert sind. Bereits 2008 hatte die American Civil Liberties Union (ACLU) diese Zone als von Verfassungsrechten „bereinigt“ („Constitution Free Zone“) bezeichnet. Zoll- und Grenzschutzbeamte haben hier das Recht, anlasslos Durchsuchungen durchzuführen.[61] Ebenfalls anlasslos darf Privatbesitz (bis auf Wohnungen) im Abstand von bis zu 25 Meilen entlang jeder Grenze durchsucht werden[62] – auch unter Zuhilfenahme von Drohnen.[63] 2014 muss die Grenzschutzbehörde zugeben, ihre Predator-Drohnen 700mal an andere Behörden zur Inlandsüberwachung verliehen haben.[64] Die Grenz- mutiert so zur Heimatdrohne.[65]

Grenzraum Mittelmeer

Insoweit Arizona das Laboratorium ist, in dem – unter direktem Bezug auf die Erfahrungen des israelischen Militärs – ein technologiebasiertes US-Grenzregime rund um Drohnen ausgebaut wird, stößt es in der EU auf großes Interesse. Was der US-amerikanischen Regierung ihre Wüstenregion, ist den Schengen-Staaten ihr Mittelmeer: Militarisiertes Experimentierfeld für Migrantenmanagement durch Technologie.

260.000 Personen stellten im Jahr 2010 in den EU-Mitgliedsstaaten einen Asylantrag, rund 10.000 davon kamen über das Mittelmeer, 2014 waren es laut UNHCR-Angaben 866.000 Antragssteller, darunter 570.800 in EU-Mitgliedsstaaten; 219.000 von ihnen flohen über das Mittelmeer.[66] Auch nachdem die Landesgrenzen weitgehend mit Zäunen, Sensortechnologien und aufgerüsteten Grenztruppen abgeschottet sind, erreichen also immer noch drei Viertel aller Flüchtenden die „Festung Europa“ auf dem Landweg, und wie in den USA steigt die Zahl der Flüchtenden (und Toten), trotz des Ausbaus der Grenzräume und der Verlagerung in Drittstaaten, die, wie Libyen, mit Grenzdrohnen ausgerüstet werden.[67]

Vor dem Maastricht-Vertrag von 1992 haben Grenzfragen einen noch vorwiegend von Wirtschaftsregulation und Logistiksicherung (spätere 1. Säule, Gemeinschaft) sowie von Gemeinsamer Außen- und Sicherheitspolitik (2. Säule, GASP) geprägten Charakter. Auch wenn die Zahl der Asylanträge in der EU sich 1992 auf 670.000 beläuft,[68] werden Grenzfragen maßgeblich durch Wirtschafts-, Außen- bzw. Verteidigungsministerien behandelt; die 3. Säule (Justiz, Inneres) konsolidiert sich erst mit dem Vertrag von Amsterdam (1997). Mit dem Schengen Catalogue von 2002[69] und mit dem Vertrag von Lissabon (2007) zerfallen die drei Säulen, auch wenn die GASP eine eigenständige Rolle behält. Grenzfragen werden zu einer Sache der Innenministerien und eskalieren mit 9/11 auch in Europa zu einer sich militarisierenden Angelegenheit. Für das Schengen-Europa rücken unter diesem Eindruck nun ebenfalls Grenzdrohnen ins Blickfeld.

Ausdruck davon sind der Strategic Aerospace Review for the 21st Century (2002), der von einer Advisory Group vorgelegt wurde und erstmals Drohnen thematisiert, die Sicherheitsstrategie der Europarats Research for a Secure Europe (2004) durch die Group of Personalities, ein ebenfalls von der Europäischen Kommission ernanntes Gremium, das mehrheitlich mit Vertretern der Militärindustrie besetzt war und erstmals Drohnen für zivile und militärische Nutzung thematisierte.[70] Im 5. Rahmenprogramm (1998-2002) werden unter der Führung von Israel Aircraft Industries 7,5 Mill. Euro für Drohnen-„Visionen“[71] bereitgestellt, im FP 6 (2002-2006) wurden 62 Mill. Euro für Überwachungstechnologie ausgereicht, darunter für die Projekte LIMES (21 Mill. Euro)[72] und µDRONES (1,9 Mill. Euro).[73] Im aus der Sicherheitsstrategie resultierenden Forschungsprogramm zur zivilen Sicherheitspolitik, Prepatory Action for Security Research (2004-2006) werden die ersten Drohnenprojekte umgesetzt.[74] Im folgenden FP 7 (2007-2013) gehen von rund 230 Mill. Euro für „Intelligente Überwachung und Grenzsicherheit“[75] 25,9 Mill. an Drohnenprojekte,[76] die Gesamtsumme für Drohnenforschung beträgt 119,8 Millionen.[77] Im Gesamtbudget von Horizon 2020 (2014-2020) sind rund 63 Mill. Euro für „Secure Societies“ vorgesehen, davon sollen zwischen 18 und 37 Millionen an drohnenrelevante Grenzsicherungsprojekte ausgereicht werden.[78]

2005 beginnt FRONTEX, die europäische Grenzschutzorganisation, ihre Tätigkeit als Koordinator der Mitgliedsstaaten, sie führt Risikoanalysen durch, entwickelt Pilotprojekte, organisiert Workshops und Demonstrationsprojekte. 2015 hat Frontex 256 Beschäftigte (2007: 82) und ein Budget 115 Mill. Euro (35 Mill.). Allein zwischen 2010 und 2014 finden 18 Veranstaltungen zu Flugdrohnen und deren Subsystemen statt,[79] für die Frontex an die eingeladenen Drohnen- und Subsystemproduzenten jeweils bis zu 200.000 Euro zahlt.[80] Frontex versteht sich nicht nur als „Schlüsselinstitution, um die Lücke zwischen Produzenten und Endabnehmern zu schließen“,[81] sondern setzt Standards für Kapazitäten, die Drohnen haben sollen[82] und erwägt, selbst Drohnen anzuschaffen.[83]

Weil derzeit in Europa (und den USA) keine Richtlinien für den Flug unbemannter Systeme in größerer Höhe und von größerem Gewicht vorliegen, beruhen Drohneneinsätze bisher auf Ausnahmegenehmigungen;[84] bis Dezember 2015 will aber die EU (die USA bis 2016) verbindliche Flugregeln aufstellen.[85] „Echte“ Drohneneinsätze über dem Mittelmeer haben bisher nur das spanische und italienische Militär (während der Operation Mare Nostrum) geflogen;[86] dabei auch in libyschen und maltesischen Hoheitsgewässern.[87] Das italienische Militär überwachte den libyschen Hafen in Tripolis zuletzt im Februar 2015 mit einer Predator A+[88] und begann im März mit der Mission Mare Sicuro, die italienische Bohrinseln in libyschen Gewässern mit Predator B überfliegt.[89] Auch für Frontex ist die Erstellung von common pre-frontier intelligence pictures, also die Ausspähung von Nicht-Schengen-Staaten, Teil des Aufgabenspektrums.[90] Ab 2016 soll die Integration von Drohnen in das europäische system of systems möglich sein.

Was den USA ihre Secure Border Initiative war, ist der EU-Kommission ihr Projekt European Border Surveillance System (EUROSUR). Von der EU-Kommission seit 2008 entwickelt

und im Oktober 2013 bewilligt, werden technologiebasiert Frontex und die Nationalen Koordinierungszentren (NCC) der Grenzüberwachung so vernetzt, dass echtzeitnaher Informationsaustausch inklusive Verteilen, Speichern, Bearbeiten und Weiterverbreiten von Daten aus einer Vielzahl von Quellen und an eine Vielzahl von Adressaten möglich wird.[91] Wo Forschungslücken bestehen, werden sie durch Horizon 2020 gefüllt.[92] Auch hier dominiert die Rüstung, elf von 13 Projekten wurden bzw. werden von Militärfirmen geführt.[93] Doch EUROSUR ist nicht allein.

Maritimes Situationsbewusstsein[94]

Ähnlich wie in den USA konkurrieren unterschiedliche Systeme um den Status als system of systems. Man ist sich zwar einig, dass „irreguläre" Migranten und Flüchtlinge unerwünscht sind, aber welche Technologie sich durchsetzt, welche Drohnen zum Einsatz kommen, welche Rüstungs- und Technologiefirmen vom Grenz- und Migrationsmanagement profitieren, das bleibt polit-ökonomisch umkämpftes Terrain.

Hinter dem European Border Surveillance System (EUROSUR) stehen maßgeblich die Generaldirektion Migration und Inneres (GD Home) und Frontex. Zwei weitere, mit einem „Facebook approach"[95] arbeitende, Systeme sind das militärische Maritime Surveillance System (MARSUR), das von der Europäischen Verteidigungsagentur (EDA) betrieben wird, und das Common Information Sharing Environment (CISE) der aus der früheren 1. Säule stammenden Generaldirektion für maritime Angelegenheiten und Fischerei (GD Mare), in der militärische und zivile Agenturen zusammenarbeiten. Drohnen hätten alle gern, dabei aber auch die Führerschaft innerhalb der EU, so dass konkurrierend zueinander und mit jeweils unterschiedlichen Unternehmen gearbeitet wird – das bevorzugte Testfeld ist das Mittelmeer.

Frontex und verschiedene Anrainerstaaten beginnen im Mittelmeer mit ersten Drohnentesteinsätzen im Rahmen der Projekte Closeye (ab Juli 2015) und Sunny (September 2016).[96] Die GD Mare gibt 2015 bekannt, sie erwäge den Kauf von Drohnen,[97] während das Gemeinschaftsprojekt der Europäischen Weltraum- (ESA) und Verteidigungsagentur (EDA), DeSIRE,[98] seine Drohnentestflüge bereits Ende 2014 absolvierte und in eine zweite Phase getreten ist. Mit dem Projekt Aeroceptor (Sommer 2015), das im FP 7 bewaffnete Drohnen für den Einsatz gegen Fahrzeuge und Boote testet und an dem die Innenministerien bzw. Polizeien Spaniens und Israels beteiligt sind, wird auch in Europa die Grenz- zur Heimatdrohne.[99] Am 19. Mai 2015 schließlich unterzeichnen die Verteidigungsminister von Frankreich, Deutschland und Italien ein Abkommen zur Entwicklung einer bewaffneten Flugdrohne bis 2025 und folgen damit der Aufforderung der Firmen Airbus Defence, Dassault Aviation and Finmeccanica vom Juni 2013 und Mai 2014, ein System zu entwickeln, „for both military and security missions".[100]

Das Beispiel USA zeigt, Migranten oder Flüchtlinge lassen sich mit dem vorhandenen Drohnenarsenal bzw. seinen Subsystemen und sonstigem Militärmaterial nicht aufhalten. Im Ergebnis „sehen" die Grenzschutzbehörden mehr – auch mehr Tote – und die Drohnen- und Rüstungsfirmen mehr Umsatz. Über dem Mittelmeer drängt die EU jetzt entschlossen auf den militärischen Einsatz. Die EU-Kommission erwartet dazu vom UN-Sicherheitsrat kurzfristig ein Mandat, denn im Juni 2015 soll ihre dreistufige Mission EU Navfor Med beginnen, die „in der Endphase die „Neutralisierung" von Schleuserbooten, Treibstofflagern und sonstigen Einrichtungen vorsieht".[101]

„Prävention durch Abschreckung", auf diese Formel haben vor zwanzig Jahren die USA ihre Politik gegen Flüchtlinge gebracht, in Europa will man zum Sommer hin, so muss man die angekündigten signature strikes europäischer Prägung wohl verstehen, im südlichen Mittelmeer auf sie schießen. Man reibt sich die Augen – und das Führungspersonal der Drohnen- und Rüstungskonzerne sich die Hände.

1 Man spricht von ›Systemen‹, wenn neben der Drohne auch die Steuereinheit gemeint ist; in den USA ist der Begriff ›Unmanned Aerial Vehicle System‹ (UAVS) gebräuchlich, in der EU ›Remotely Piloted Aerial System‹ (RPAS).

2 J. Stewart, Marine Corps Considers New Unmanned Tank, Micro-Drones (30.01.15), http://www.marinecorpstimes.com/.

3 I. Lapowsky, Facebook Lays Out Its Roadmap for Creating Internet-Connected Drones (23.09.14), http://www.wired.com/.

4 Vgl. P.W. Singer, Wired for War. New York 2009; Deutscher Bundestag, Stand und Perspektiven der militärischen Nutzung unbemannter Systeme (Drucksache 17/6904). Berlin 2011.

5 Vgl. für viele Frost & Sullivan, The Future of Drones. London 2015.

6 D. Cenciotti, nEUROn Stealth UCAV has Started Testing its Advanced Sensors in Italy (16.04.15), http://theaviationist.com/.

7 V. Eick, ›Dieser Frieden ist uns Krieg genug‹. In. R. Bauer (Hg.), Kriege im 21. Jahrhundert. Anweiler am Trifels 2015: 174.

8 Ebd.: 169.

9 So China, Deutschland, Frankreich, Großbritannien, Iran, Israel, Italien, Libanon, Russland, Schweden, Taiwan, Türkei, USA; Indien und Pakistan haben die Bewaffnung angekündigt, vgl. M. Zenko & S. Kreps, Limiting Armed Drone Proliferation. New York 2014. Die US-Streitkräfte, derzeit im Besitz von über 11.100 Flugdrohnen, klagen über Produktionsengpässe, vgl. J. Sciutto, Drone Shortage Threatens War on ISIS (18.11.14), http://edition.cnn.com/.

10 Rand Corporation, Armed and Dangerous? UAVs and U.S. Security. Santa Monica 2014: 7-9.

11 European Parliamentary Research Service, Use of Armed Drones. Strasbourg 2014.

12 G. Arnett, The Numbers Behind the Worldwide Trade in Drones. The Guardian, 17.03.15.

13 Erstmals wurden bewaffnete Drohnen 2007 exportiert (Großbritannien erhält zwei MQ-9 Reaper aus den USA). China war 2014 das zweite Land (Lieferung von fünf bewaffneten Drohnen an Nigeria); vgl. M. Rajagopalan, Eyeing Exports, China Steps Up Research into Military Drones (29.04.15), http://www.reuters.com/.

14 Woher die Bezeichnung ›Drohnen‹ oder ›drones‹ für die fliegenden unbemannten Systeme stammt, ist strittig; vgl. Eick 2015, a.a.O.: 172f.

15 Die meisten der von der US-amerikanischen Zoll- und Grenzpolizei (Customs and Border Protection) eingesetzten Drohnen können aus einer

Höhe von bis zu vier Kilometern etwa die Farbe von Kleidung unterscheiden; vgl. UPI, Drones Spying on Mexico? (21.11.2010), http://www.upi.com/.

16 G. Coppola & B. Schmidt, World Cup Drones From Tel Aviv Bring Fall of Rio Kingpin (16.06.14), http://www.bloomberg.com/.

17 A. Becker, New Drone Radar Reveals Border Patrol ›Gotaways‹ in High Numbers (04.04.13), http://cironline.org/.

18 C. Drew, Drones Are Weapons of Choice in Fighting Qaeda. New York Times, 17.03.09. In Afghanistan verloren die US-Streitkräfte zwischen 2001 und 2003 sechs der dort eingesetzten zwölf Predators und zwei Global Hawk, vgl. C. Whitlock, When Drones Fall from the Sky. The Washington Post, 20.06.14; zu Unfällen im Inland, vgl. C. Whitlock, Near-Collisions between Drones, Airliners Surge. The Washington Post, 26.11.14.

19 Bundeswehr, Übersicht: Drohnen der Bundeswehr und Drohnenverluste (Stand: 25.06.14).

20 Zu den Lobby-Netzwerken der Drohnenmärkte gehören auf internationaler Ebene seit 1999 das sich heute AUVS International (AUVSI) nennende Netzwerk mit 2.700 Mitgliedern aus über 60 Ländern, in der EU die UAV DACH (Deutschland, Italien, Niederlande, Österreich, Schweiz), in denen jeweils Vertreter von Unternehmen, aus dem akademischen Bereich und (para)staatlichen Institutionen vertreten sind; vgl. V. Eick, Das Dröhnen der Drohnen. Bürgerrechte & Polizei/CILIP 94(3) 2009: 37ff; E. Töpfer, Die Himmelsstürmer. FifF 11(4) 2011: 31; Statewatch, Drone Inc. London 2014: 10-25.

21 European Security Research Advisory Board, Meeting the Challenge. Luxembourg 2006: 30.

22 In Deutschland ist es das vom Bundesforschungsministerium koordinierte Programm ›Forschung für die zivile Sicherheit‹. Es wäre irreführend, den Begriff ›zivil‹ wörtlich zu nehmen: Bei seiner Einrichtung hieß es, es „befasst sich nicht mit militärischer Sicherheitsforschung“, vgl. Bundesministerium für Bildung und Forschung, Forschung für die zivile Sicherheit. Berlin 2007: 11. Drei Jahre später, das „in der militärischen Forschung erworbene technologische Know-how muss auch im Bereich der zivilen Sicherheitsforschung verfügbar sein und umgekehrt“; vgl. K. Thoma et al., Positionspapier des wissenschaftlichen Programmausschusses zum nationalen Sicherheitsforschungsprogramm. Freiburg/Brsg. 2010: 7.

23 Statewatch 2014, a.a.O.: 27.

24 European Commission, Towards a European Strategy for the Development of Civil Applications of Remotely Piloted Aircraft Systems (RPAS), Brussels 2012: 4.

25 L. Marin, Is Europe Turning into a ›Technological Fortress‹? In: M.A. Heldeweg & E. Kica (eds.), Regulating Technological Innovation. New York 2011; R. Nieto-Gomez, Walls, Sensors, Drones. In: E. Vallet (ed.), Border, Fences and Walls. Farnham/UK 2014.

26 Zum Begriff ›Pazifizierung‹, vgl. V. Eick & K. Briken (eds.), Urban (In) Security. Ottawa 2014.

27 T. Gammeltoft-Hansen & N. Nyberg Sorensen, Migration Industry and the Commercialization of International Migration. New York 2013.

28 N.A. Naples & J. Bickham Mendez (eds.), Border Politics. New York 2015.

29 Die Grenze zu Texas ist ca. 2.000 km lang (zu New Mexico: 280 km; Kalifornien: 230 km).

30 Für die ersten massenhaften Deportationen nach dem II. Weltkrieg vgl. aber J.R. García, Operation Wetback. Westport/CT 1980.

31 ACLU, Customs and Border Protection’s 100-Mile Rule. Washington D.C. 2015.

32 T. Dunn, The Militarization of the U.S.-Mexico Border 1978-92. Austin/TX 1996.

33 Nieto-Gomez 2014, a.a.O.: 195.

34 Ebenda: 196.

35 T.J. Dunn & J. Palafox, Militarization of the Border. In: S. Oboler & D.J. González (eds.), The Oxford Encyclopaedia of Latinos and Latinas in the United States. Oxford 2005

36 G. Boyce, Shooting in the Dark (22.05.13), https://nacla.org/print/9071.

37 Department of Homeland Security, Integrated Surveillance Intelligence System, http://www.globalsecurity.org/.

38 Nieto-Gomez 2014, a.a.O.: 201.

39 Department of Homeland Security, Report on the Assessment of the Secure Border Initiative-Network (SBInet) Program. Washington D.C. 2011.

40 K. Johnson, Homeland Security Scraps Border Fence. Wall Street Journal, 15.01.11.

41 T. Barry, Drones Over the Homeland. Washington D.C. 2013: 7-11.

42 J. Napolitano, zit.n. Johnson 2011, a.a.O.

43 Office of Inspector General, A Review of Remote Surveillance Technology Along U.S. Land Borders. Washington D.C. 2005: 13f. Etwa zeitgleich schließt auch die mexikanische Regierung einen Vertrag mit Elbit ab und kauft mindestens eine Drohne für die Grenzüberwachung. 2009 folgen Verträge mit der israelischen Firma Aeronautics Defense Systems über 22,5 Mill. US-Dollar für Drohnen des Typs Orbiter und Skystar 300, J. Johnson, A Palestine-Mexican Border (29.06.12), https://nacla.org.

44 J. Blazakis, Border Security and Unmanned Aerial Vehicles, Washington D.C. 2004: 1-3.

45 G. Thompson & M. Mazzetti, U.S. Drones Fight Mexican Drug Trade. New York Times, 15.03.11.

46 Defense Update, CBP Awards $145 Million Border Towers Contract to Elbit (02.03.14), http://defense-update.com/.

47 Barry 2013, a.a.O.: 6.

48 D. Iaconangelo, Border Patrol VADER. Los Angeles Times, 20.06.13.

49 Becker 2013, a.a.O.

50 Ursprünglich waren es elf Drohnen, doch zwei stürzten im April 2006 bzw. Januar 2014 ab, vgl. Department of Homeland Security, U.S. Customs and Border Protection’s Unmanned Aircraft System Program Does Not Achieve Intended Results. Washington D.C. 2014: 2.

51 SAR vergleicht automatisiert zweidimensionale Bilder von Gelände im Zeitverlauf, etwa um frische Fuß- oder Reifenspuren zu identifizieren.

52 Statt 16 Stunden pro Tag in der Luft zu sein, fliegen sie durchschnittlich nur 3,5 Stunden; das Grenzgebiet ist, anders als angekündigt, nicht vollständig abgedeckt; VADER fliegt nur Teile der Grenze Arizonas ab; strittig ist, welchen Anteil die Drohnen an den gestiegenen Festnahmezahlen haben; die Kosten haben sich nicht reduziert.

53 T. Payan, The Three U.S.-Mexico Border Wars: Drugs, Immigration, and Homeland Security. Westport/CT 2006: 68f; R. Balko, Rise of the Warrior Cop. New York 2013.

54 Von den 4.400 Toten der vergangenen zehn Jahre (2004-2014) starben die Hälfte im Grenzsektor Tucson (Arizona), ein weiteres Viertel im Rio Grande Valley (Texas). Die Zahl der Toten ist in den vergangenen 20 Jahren kontinuierlich gestiegen, vgl. United States Border Patrol, Southwest Border Deaths By Fiscal Year. Washington D.C. 2015.

55 Nieto-Gomez 2014, a.a.O.: 204; Arizona

Advisory Committee, Tragedy Along the Arizona-Mexico Border. Washington D.C. 2002: 1f. 56 Department of Homeland Security, US-Mexico Border Fence/ Great Wall of Mexico Secure Fence. Washington D.C. 2012, http://www.globalsecurity.org/.

57 Insgesamt sind 7,25 Mrd. US-Dollar für die Grenzsicherung vorgesehen, vgl. US Senate, Border Security, Economic Opportunity and Immigration Modernization Act 2013. Washington D.C. 2013: SEC. 5, C ii, SEC. 1102.

58 „Additional payload upgrades could include expendables or non-lethal weapons designed to immobilize TOIs“ (TOIs – targets of interest), vgl. Department of Homeland Security, Concept of Operations for CBP's Predator B Unmanned Aircraft System. Washington D.C. 2010: 63.

59 E. Spagat & B. Skoloff, Drones Patrol Half Of Mexico Border, The Huffington Post, 13.11.2014.

60 US Senate 2013, a.a.O.: SEC. 1101-3.

61 Vgl. die Entscheidung von 1973, Almeida-Sanchez v. United States (8 C.F.R. § 287.1(b)).

62 ACLU 2013, a.a.O.

63 Thompson 2013, a.a.O.: 12ff; ACLU, Protecting Privacy from Aerial Surveillance. New York 2011.

64 M. Peck, Drones Can't Protect Our Borders (16.01.15), http://nationalinterest.org.

65 Für Beispiele zum Heimateinsatz von Drohnen durch Polizei und Militär in den USA seit 2011 vgl. Eick 2015, a.a.O.: 192ff; Tyler Wall, Unmanning the Police Manhunt. Socialist Studies 9(2) 2013; für getestete Bewaffnung vgl. D. Murphy & J. Cycon, Applications for Mini VTOL UAV for Law Enforcement. San Diego/CA 1998.

66 UNHCR, Asylum Trends 2014. Geneva 2015.

67 Amnesty International, Submission to the Council of Europe Committee of Ministers: Hirsi Jamaa and Others v. Italy (Application No. 27765/09). Brussels 2014: 5.

68 Forschungsgruppe ›Staatsprojekt Europa‹ (Hg.), Kämpfe um Migrationspolitik. Bielefeld 2014.

69 Council of the European Union, EU Schengen Catalogue. External Borders Control, Removal and Readmission. Brussels 2002.

70 European Commission, Research for a Secure Europe. Luxembourg 2004: 20.

71 U.a. für die Projekte CAPECON, USICO, UAV-NET, HELIPLAT, vgl. Töpfer 2011, a.a.O.: 31.

72 Satellitenüberwachung, u.a. für die Frontex Joint Operation Nautilus vor Libyen 2006ff, vgl. G. Cannizzaro, The LIMES and G-MOSAIC EC Integrated Projects to Support Security Management in EU. Rome 2009: 2f.

73 Überwachung urbaner Umgebungen mit Kleinstdrohnen, vgl. D. Bigo & J. Jeandesboz, Review of Security Measures in the 6th Research Framework Programme and the Preparatory Action for Security Research. Paris 2008: 7.

74 V. Boulanin & R. Bellais, Towards a High-Tech ›Limes‹ on the Edges of Europe? In: E. Vallet (ed.), Border, Fences and Walls. Farnham/UK 2014: 239; Eick 2009, a.a.O.: 38.

75 D. Bigo, J. Jeandesboz, M. Martin-Maze, F. Ragazzi, Review of Security Measures in the 7th Research Framework Programme. Brussels 2014: 25.

76 Darunter OPARUS (1,2 Mill. Euro), TALOS (12,9), WIMA2S (2,7), vgl. European Commission, Investing Into Security Research for the Benefits of European Citizens. Brussels 2010: 102f, 148f, 158f.

77 Statewatch 2014, a.a.O.: 38; die EU-Kommission bezweifelt diese Angaben, vgl. European Commission, E-008990 14. Brussels 2014.

78 European Commission, Horizon 2020 (14. Secure Societies). Brussels 2015: 73-84.

79 K. Krajčíková, Drones' Deployment by FRONTEX and Fundamental Rights and Civil Liberties. Twente 2014: 11-13, 30f.

80 A. Fotiadis & C. Ciobanu, Closing Europe's Borders Becomes Big Business (09.01.13), http://oppenheimer.mcgill.ca/.

81 Frontex, Role, http://frontex.europa.eu/research/role/.

82 L. Marin & K. Krajčíková, Deploying Drones in Policing European Borders. In: A. Završnik (ed.), Drones and Unmanned Aerial Systems. Heidelberg 2015: 9.

83 Daniel Deibler, EUROSUR – A Sci-fi Border Zone Patrolled by Drones? In: J. Camenisch, S. Fischer-Hübner, M. Hansen (eds.), Privacy and Identity Management for the Future Internet in the Age of Globalisation. Heidelberg 2015: 95.

84 FAA, Authorizations Granted Via Section 333 Exemptions (15.05.15), https://www.faa.gov/uas/.

85 G.S. McNeal, European Drone Regulations are about to Get Smarter and More Permissive (23.03.15), http://www.forbes.com/.

86 Ebenso die Schweiz in 2011 (an der Grenze zu Italien), vgl. L. Marin, The ›Metamorphosis‹ of the Drone. In: D. Bowman, A. Rip, E. Stokes (eds.), Embedding and Governing New Technologies. Singapore 2015: 4, 11, 13.

87 S. Carrera & L. den Hertog, Whose Mare? Rule of Law Challenges in the Field of European Border Surveillance in the Mediterranean. Brussels 2015: 4.

88 D. Cenciotti, MQ-1C Predator Filmed Italian Repatriation (16.02.15), http://theaviationist.com.

89 T. Kington, Italy Wants Bombing of Libya to Halt Migrants. The Times, 16.04.15.

90 N. Nielsen, Frontex Chief Looks Beyond EU Borders (14.01.13), https://euobserver.com/.

91 Jan Mulder, Report on the Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR). Brussels 2014. Zusammengearbeitet werden soll dabei auch mit Drittstaaten, auch den Herkunftsländern der Flüchtlinge und Migranten, vgl. Deibler 2015, a.a.O.: 98.

92 Vgl. European Commission 2015, a.a.O.: 77.

93 Heinrich Böll Stiftung, Borderline. The EU's New Border Surveillance Initiatives. Berlin 2012: 59-64.

94 Europäische Kommission, Auf dem Weg zur Integration der Meeresüberwachung. Brüssel 2009: 2.

95 Carrera & Den Hertog 2015, a.a.O.: 18.

96 European Commission, E-007958-14. Brussels 2014; European Commission, E-007959-14. Brussels 2014.

97 European Maritime Safety Agency, Maritime Surveillance in Practice. Lisbon 2015: 6.

98 DeSIRE (Demonstration of Satellites enabling the Insertion of RPAS in Europe), vgl. https://artesapps.esa.int/projects/desire.

99 European Commission, E-007499-13. Brussels 2013.

100 Airbus, Finmeccanica and Dassault Aviation Welcome European MALE Study (19.05.15), http://www.uasvision.com/.

101 A. Rettman, EU Countries Agree Boat-Sinking Operation (18.05.15), https://euobserver.com/.

Matthias Monroy

Grenzen sind nicht intelligent

Neues zur geplanten Superdatenbank „Smart Borders“

Seit 2008 planen die Mitgliedstaaten der Europäischen Union die Einführung einer neuen Vorratsdatenspeicherung von allen Reisenden aus „Drittstaaten“[1]. 2011 mündeten die Vorbereitungen schließlich in einer Mitteilung der EU-Kommission[2] und haben seitdem einen Namen: „Intelligente Grenzen“ („Smart Borders“). Das Gesamtpaket besteht aus zwei Säulen. In einem „Ein-/Ausreisesystem“ („Entry/Exit System“, EES) werden die Ein- und Ausreisen aller Drittstaatsangehörigen erfasst – unabhängig davon, ob diese ein Visum für den Schengen-Raum benötigen oder nicht. Die betroffenen Reisenden werden mithilfe ihrer Fingerabdrücke oder dem Scan ihrer Iris identifiziert und gespeichert. Sofern die Daten nicht aus biometrischen Reisedokumenten ausgelesen werden können, werden sie vor Ort abgenommen. Doch es geht auch bequemer: „Drittstaatsangehörige mit niedrigem Risikoprofil“ können sich in einem „Registrierungsprogramm für Reisende“ („Registered Travellers Programme“, RTP) vorab in den konsularischen Vertretungen oder den geplanten gemeinsamen Visastellen überprüfen lassen und persönliche sowie biometrische Daten hinterlegen. Mit diesem Privileg dürfen dann automatisierte Kontrollgates genutzt werden. Voraussetzung ist unter anderem der Nachweis „ausreichender Existenzmittel“ und der Besitz eines biometrischen Passes.

Geführt würde die neue Datensammlung bei der im Dezember 2012 in Estland eingerichteten Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA)[3]. In einer Mitteilung von 2010[4] schrieb die Kommission, Ziel der Maßnahmen sei es, „eine weltoffene Union zu wahren, gleichzeitig aber die illegale Einwanderung und das organisierte Verbrechen zu bekämpfen“. Besonders haben es die InnenministerInnen der Europäischen Union auf so genannte „Overstayer“ abgesehen. Gemeint sind MigrantInnen, die zunächst mit einem gültigen Aufenthaltstitel in die EU einreisen, den Schengen-Raum aber nicht fristgemäß wieder verlassen. Zwar werden ihre Ein- und Ausreisen in den meisten Mitgliedstaaten schon protokolliert. Die Systeme sind aber nicht grenzüberschreitend vernetzt. Es kann also nicht festgestellt werden, ob eine Person, die über den Flughafen Frankfurt einreiste, längst über eine EU-Außengrenze wieder ausgereist ist. Mindestens 14 Mitgliedstaaten verfügen bereits über ein nationales Ein- und Ausreisesystem. Hierzu gehören Spanien, Litauen, Polen, Rumänien, Bulgarien, Zypern, Portugal und Großbritannien. Womöglich können die Systeme später in die geplante europäische Plattform integriert werden.



Erste Fingerabdrücke, die William James Herschel (1833-1917) in den Jahren 1859 und 1860 fertigte. Quelle: Wikimedia Commons

Liegt eine verspätete Ausreise vor, soll das „Ein-/Ausreisesystem" eine Meldung ausgeben. Bislang ist nicht die Rede davon, dass dann sofort eine Fahndungsausschreibung im Schengener Informationssystem (SIS) angelegt würde. Vielmehr geht es um buchhalterische Zahlen und Statistiken für eine „faktenbasierte Politik". Werden etwa zu viele „Overstayer" festgestellt, können Folgemaßnahmen ergriffen werden.

Milliardenschweres Paket

Besonders das „Registrierungsprogramm für Reisende" soll aber auch die Handhabung wachsender „Reiseströme an den Grenzen" verbessern. Laut dem Verordnungsvorschlag der EU-Kommission von 2011 wurden die Außengrenzen der damals 27 EU-Mitgliedstaaten jährlich rund 700 Millionen Mal übertreten. Ein Drittel aller Einreisen werden „Drittstaatsangehörigen" zugeschrieben. Allein für den Luftverkehr wird bis 2030 von einer Zunahme von 400 auf rund 720 Millionen Reisende ausgegangen. Der Umfang der neuen Vorratsdatenspeicherung wäre immens: Die Kommission rechnet mit jährlich rund 269 Millionen Reisenden.

Für beide Projekte der Initiative „Intelligente Grenzen" waren im Vorschlag von vor vier Jahren 1,35 Milliarden Euro kalkuliert. Die EU-Kommission hat noch keine Übersicht über ihre Verteilung auf den EU-Haushalt bzw. die Haushalte der Mitgliedstaaten vorgelegt. Die jährlichen Betriebskosten gab die Bundesregierung in der Antwort auf eine Kleine Anfrage mit 88 Millionen Euro für das EES bzw. mit 101 Millionen Euro für das RTP an[5]. Dies deckt sich mit Angaben der Kommission, die Unterhaltskosten von jährlich 190 Millionen Euro in den ersten fünf Jahren vorsieht. Technisch muss gelöst werden, wie EES und das RTP mit anderen Datensammlungen kommunizieren und welche zusätzlichen Kosten dafür veranschlagt werden müssten. Denn alle Zugangspunkte sollen unter den 28 EU-Mitgliedsstaaten kompatibel sein. Nicht absehbar ist auch, ob die tatsächlichen Kosten für das Gesamtpaket nicht deutlich steigen: Der Upgrade des Schengener Informationssystems (SIS) auf die Version SIS II war beispielsweise 13 Mal teurer als geplant.

Bereits existierende Datenbestände könnten laut dem Bundesinnenministerium mit dem „Ein-/Ausreisesystem" und dem „Registrierungsprogramm für Reisende" kombiniert werden. Möglich wäre die Integration des Schengener Informationssystems, der biometrischen Datenbank EURODAC oder des Visa-Informationssystems. So würden auch von „Drittstaatenangehörigen" besuchte Orte, WohnungsgeberInnen oder Transportmittel in die Datenverarbeitung eingebunden. Wird auch die nach gegenwärtigem Stand geplante EU-Fluggastdatensammlung eingebunden, entsteht eine Superdatenbank mit unabsehbaren Konsequenzen für das Prinzip der Datensparsamkeit.

Öffnung auch für die Strafverfolgung? Polizeibehörden wollen zehn Fingerabdrücke

Viele Mitgliedsstaaten hatten wegen der Kosten Bedenken angemeldet. Die Zahl der mit den Systemen aufgespürten „Overstayer" dürfte mit den milliardenschweren Ausgaben kaum im Verhältnis stehen: Laut Bundesregierung hat die Bundespolizei 2010 lediglich 5.405 Personen festgestellt, deren Visum bzw. Aufenthaltstitel abgelaufen war. Fünf Jahre zuvor waren es noch 7.454. Die Unverhältnismäßigkeit des Pakets „Intelligente Grenzen" führt aber nicht zu dessen Abbruch, sondern sogar zu dessen Ausweitung. Nicht nur die Bundesregierung setzt sich dafür ein[6], außer der Grenzpolizei auch anderen anderen Polizeibehörden Zugang zu gewähren. Nur wenn es auch zur Gefahrenabwehr und Strafverfolgung genutzt werden dürfe, seien die hohen Ausgaben gerechtfertigt, das System mithin rentabel[7]:

> *Eine Reihe von Mitgliedstaaten äußerte Zweifel am Kosten-Nutzen-Verhältnis, wenn das EES nicht auch zur Verhütung und Verfolgung terroristischer und sonstiger schwerwiegender Straftaten genutzt werden könne.*

Die Öffnung des Systems für die Strafverfolgung würde aber selbst höhere Kosten verursachen, denn die Polizeibehörden drängen darauf dass möglichst nicht nur vier, sondern alle zehn Fingerabdrücke abgenommen werden.

Im Herbst hatte die Kommission Ergebnisse einer Machbarkeitsstudie vorgelegt[8], die verschiedene technische Konzepte untersucht und bewertet hat. Dabei ging es auch um die Zahl der abgenommenen Fingerabdrücke. Abgewogen wurden aber auch die Kosten für Serverkapazitäten, die je nach Datengröße variieren. Die Kommission gibt die Mindestgröße von Gesichtsbildern mit 15 kb an, zehn Fingerabdrücke belegten demnach mindestens 120 kb. Würden nur vier Fingerabdrücke verarbeitet, fielen deutlich weniger Speicherbedarf und Bandbreite zur Übertragung an.

Ebenfalls noch unklar ist der Umfang der verarbeiteten Daten. In der Technischen Studie der Kommission heißt es, die grenzpolizeilichen Zwecke erforderten lediglich die Erhebung von 26 Datenfeldern. Der ursprüngliche Vorschlag zur Errichtung des „Intelligente Grenzen" schlug 36 Datenfelder vor, darunter außer den Personendaten und biometrischen Daten auch solche zu Reisedokumenten, Visa, früheren Ein- und Ausreisen oder Verlängerung von Aufenthaltserlaubnissen. Dokumentiert würde auch wann und wo die Europäische Union betreten oder verlassen wird. Nehmen die Reisenden das „Registrierungsprogramm für Reisende" in Anspruch, werden auch die dort erhobenen Antragsdaten gespeichert. Hierzu gehören die Telefonnummer, der angegebene Reisezweck oder der Beruf. Alle anfallenden Daten könnten bis zu fünf Jahre lang gespeichert werden.

Die Einführung des Pakets „Intelligente Grenzen" bedeutet, dass an allen EU-Außengrenzen entsprechende Hardware zur Abnahme und Verarbeitung biometrischer Daten verfügbar sein müsste. Die Studie der Kommission hatte hierzu bereits problematisiert, dass dies vor allem auf Fähren, in Zügen oder an kleinen Flugplätzen ein Problem darstellt. Was die biometrische Industrie entzücken dürfte, könnte sich für Reisende nachteilig auswirken: Sollten bei der Einreise tatsächlich alle zehn Fingerabdrücke abgenommen werden, würden sich Kontrollen spürbar verlängern.

Pilotstudie im Sommer in Frankfurt

Die in der Technischen Studie beschriebenen Szenarien werden nun in

einer Pilotstudie in mehreren Mitgliedstaaten ausprobiert. Verantwortlich ist die Agentur für das Betriebsmanagement von IT-Großsystemen (eu-LISA). Auch das Bundesinnenministerium beteiligt sich daran und führt ab 22. Juni Tests am Frankfurter Flughafen durch. Zuständig ist die Bundespolizei, die für das Pilotprojekt einen Projektmanager benannt hat. Neben der Fraport AG ist auch die EU-Grenzagentur Frontex beteiligt. Getestet werden verschiedene Verfahren:



Frontex-Zentrale in Warschau
Foto: Krzysztof Zacharz, Wikimedia Commons, Lizenz: CC BY-SA 2.5

Immer wird das Gesichtsbild verarbeitet, das jedoch entweder mit vier, acht oder allen zehn Fingerabdrücken kombiniert wird. Auch bei der Abnahme der daktyloskopischen Daten kommen verschiedene Geräte zur Anwendung. So soll zum einen die an den Außengrenzen bereits existierende Technologie eingesetzt werden. Versuche werden aber auch mit der „neuesten Generation von Fingerabdruckscannern" unternommen. Hierzu gehören tragbare Geräte, die sowohl mit oder ohne direktem Kontakt der Finger funktionieren sollen. Auch die elektronischen Kontrollgates an Flughäfen und die damit womöglich verkürzten Wartezeiten werden einer Eignungsprüfung unterzogen.

Die massenhafte Erfassung und Verarbeitung biometrischer Merkmale wird bereits in mehreren EU-finanzierten Forschungsprojekten entwickelt und erprobt. Unter Leitung eines Instituts aus Österreich startete vor zwei Jahren das Projekt „Fast Pass"[9], an dem neben Grenzpolizeien auch der Flughafen Frankfurt beteiligt ist. Seit letztem Jahr führt der spanische Rüstungskonzern Indra mit „Automated Border Control Gates for Europe" (ABC4EU) ein weiteres Projekt zur automatisierten Grenzkontrolle an[10]. Hier sind vor allem Unternehmen aus biometrischen Industrie versammelt. Fast Pass und ABC4EU werden ebenfalls an den Tests in Frankfurt teilnehmen. Ihre Rolle besteht unter anderem darin, Verfahren gegen die Fälschung von Fingerabdrücken zu erproben.

Die Gesamtkosten der Pilotstudie werden mit 3,5 Millionen Euro angegeben, die dreimonatige Studie in Frankfurt soll nach derzeitigem Stand 700.000 Euro kosten. Für die Tests wird eigens eine „PC-Anwendung für die Grenzkontrolle" programmiert und in die vorhandene IT-Umgebung der Bundespolizei eingebettet. Dabei wird auch das bereits bestehende, automatisierte Grenzkontrollsystem „EasyPass" getestet und „ertüchtigt"[11]. In Deutschland sind mittlerweile 140 dieser „EasyPASS"-Stationen an den fünf passagierstärksten Flughäfen installiert. In der Pilotstudie sollen die ebenfalls an vielen Flughäfen bereits vorhandenen kontaktlosen Fingerabdruckscanner der Firma Crossmatch gegenüber Erzeugnissen der Firma Morpho getestet werden. Dabei sollen auch Reisende und Grenzbeamte nach ihren Erfahrungen befragt werden. Ergebnisse sollen im September 2015 vorliegen, im November werden diese nach jetzigem Stand in einem Abschlussbericht veröffentlicht. Dann soll sich das EU-Parlament damit befassen, damit das System „Intelligente Grenzen" zügig eingeführt werden kann. Ein Ratsdokument nennt hierfür „Mitte 2016"[12].

Das Paket „Intelligente Grenzen" ist ein System zur buchhalterischen, auf Statistiken basierenden Migrationskontrolle. Die beiden Programme fördern eine Zwei Klassen-Gesellschaft für Reisende mit mit niedrigem und hohem „Risikoprofil". Der Zugriff auch zur Gefahrenabwehr und Strafverfolgung wird die technischen Möglichkeiten von Polizeien und Geheimdiensten erneut erweitern. Die deutsche Ankündigung, die Datenbanken EURODAC, SIS oder VIS ebenfalls zu integrieren muss als Drohung verstanden werden. Denn auf diese Weise würde sich der Argwohn bewahrheiten, dass bei der Agentur für das Betriebsmanagement von IT-Großsystemen eine Super-Datenbank entsteht.

1 http://europa.eu/rapid/press-release_IP-08-215_de.htm?locale=de
2 http://europa.eu/rapid/press-release_IP-11-1234_de.htm#footnote-2
3 https://netzpolitik.org/2014/neue-it-agentur-wird-zentraler-dienstleister-von-eu-polizeidatenbanken-weiterer-aufwuchs-wird-geplant/
4 http://ec.europa.eu/atwork/pdf/cwp2011_de.pdf
5 http://dipbt.bundestag.de/dip21/btd/17/080/1708084.pdf
6 http://dip.bundestag.de/btd/18/042/1804287.pdf
7 http://dipbt.bundestag.de/dip21/btd/18/004/1800455.pdf
8 http://www.statewatch.org/news/2014/oct/eu-smart-borders-report.pdf
9 https://www.fastpass-project.eu/
10 http://abc4eu.com/
11 https://www.bundespolizei.de/DE/01Buergerservice/Automatisierte-Grenzkontrolle/EasyPass/easyPass_node.html
12 http://data.consilium.europa.eu/doc/document/ST-17060-2014-INIT/en/pdf

Dr. Andreas Höpken, Jochen Brandt

Schweigepflicht und IT-Dienstleistungen – ein Diskussionsbeitrag

Manchmal wird es Zeit sich von Unmodernem zu trennen. Neuen Platz zu schaffen scheint nicht mehr nur von Möbelhäusern propagiert zu werden, sondern auch auf gesetzliche Normen Anwendung zu finden. Eine Überprüfung des Bestehenden, mit dem Ziel den Zustand zu verbessern, ist sicher ein guter Ansatz. Fragwürdig wird es, wenn, ganz im Sinne einer Wegwerfkultur, scheinbar veraltete Regelungen abgeschafft werden sollen, die in Wahrheit noch einen Zweck erfüllen.

In diesem Beitrag geht es um die gesetzliche Norm der Schweigepflicht, den § 203 StGB. Steht sie den wirtschaftlich-technischen Notwendigkeiten (Auftragsdatenverarbeitung, Fernwartung, Cloud-Computing) in den schweigepflichtrelevanten Bereichen (Medizin, Steuerberater, Anwälte etc.) wirklich nur im Wege? Oder gibt es Möglichkeiten, beides auch im Interesse der zu schützenden Belange der Betroffenen (Patienten, Mandanten, Klienten) auf eine gesetzeskonforme Grundlage zu setzen? Dieser Beitrag versteht sich daher als Diskussionsbeitrag und nicht als finale Lösung aller Fragen. Es geht um eine alternative Zieldefinition, welche die bisherigen Beiträge um einen neuen Ansatz erweitern soll.

Schutz der Schweigepflicht versus moderne Technik

Der bayerische Landesdatenschutzbeauftragte[1] stellt die Bedrohung durch das Bekanntwerden von Daten an einem wahrhaft biblischen Beispiel dar. Im Alten Testament wird der rechtschaffene und gottesgläubige Ijob[2] Opfer einer Auseinandersetzung zwischen Gott und Satan, in dessen Folge ihn zahlreiche Krankheiten heimsuchen.[3] Hieraus resultiert für Ijob die soziale Ächtung, da sein Umfeld die Krankheiten als Strafen Gottes ansieht. Informationen über



Hiob. Darstellung von Marten Jacobsz van Veen Heemskerck. Quelle: Wikimedia Commons. Lizenz CC BY 4.0

Krankheiten sind eben immer schon sensibel gewesen und sind es heute noch. Auch wenn die Schlussfolgerungen des sozialen Umfeldes meistens andere sein werden. Es könnten – ganz banal – höhere Beiträge zur privaten Krankenkasse sein.

Was für den Bereich der Gesundheitsdaten gilt, verhält sich in den Bereichen Steuerberater, Anwälte etc. grundsätzlich nicht anders. Je nachdem, welche Daten oder Informationen hier bearbeitet werden, ergibt sich ein Gefährdungspotential für die Betroffenen, dem der Gesetzgeber in § 203 StGB Rechnung tragen will. Während der Datenschutz sich am Verbot mit Erlaubnisvorbehalt orientiert, geht die Schweigepflicht darüber hinaus. Hier reicht es für einen Verstoß gegen die Schweigepflicht aus, wenn nur die Möglichkeit besteht, dass ein Unbefugter Kenntnis der Daten erlangen könnte. Dies gilt insbesondere für alle Formen der elektronischen Datenverarbeitung.[4]

Diesem gesetzlichen Schutz steht eine immer weiter gehende Arbeitsteilung entgegen. Gerade im IT-Bereich werden immer mehr Aufgaben Spezialisten übertragen. Mittlerweile werden in vielen dieser Bereiche sogar essenzielle Datenverarbeitungsvorgänge ausgelagert. Dieses Outsourcing geht so weit, dass Daten von überall auf der Welt gewartet oder in der Cloud stehen können. Hauptargument sind dabei die Kosten bzw. der Nutzen dieser weltweiten Verwendung von Ressourcen.

Die Tatsache, dass schweigepflichtbewehrte Daten dabei von Dritten in aller Welt zur Kenntnis genommen werden könnten, wird zwar als Problem erkannt. Als Ursache des Problems wird aber das zu strenge deutsche Recht ausgemacht und nicht die Gefahren, die durch den Einsatz der Technik entstehen können.

Neuere Elemente in der Diskussion

Neue Brisanz erhält die Frage auch durch einen Vorstoß der Bundesanwaltskammer, die in der Berufsordnung für Rechtanwälte (BORA) eine Öffnung für das Outsourcing von Dienstleistungen einführen will. Die bereits beschlossene Änderung[5] bedarf noch der Genehmigung durch das Bundesministerium der Justiz und für Verbraucherschutz. Der § 2 BORA führt hier den Begriff der Sozialadäquanz ein. Sofern die in Anspruch genommenen Dienstleistungen „objektiv einer üblichen, von der Allgemeinheit gebilligten Verhaltensweise im sozialen Leben entspricht" soll kein unbefugtes Offenbaren mehr vorliegen. Offen bleibt die Frage, ob sich diese Verhaltensweise auf allgemeine Standards oder die von einem Rechtsanwalt erwarteten Standards bezieht. Ebenso bleibt die Frage offen, welche strafprozessualen Folgen sich ergeben (Hier stellen sich Fragen in Bezug auf § 53a StPO – Aussageverweigerungs-

recht und § 97 StPO – Beschlagnahmefreiheit.). Ziel dieser Änderung der BORA soll mehr Rechtssicherheit für die Anwälte sein. Aber gerade bei Anwälten dürfte die Schweigepflicht und Beschlagnahmefreiheit für den Mandanten ein besonders hohes Gut darstellen.

Einen weiteren Beitrag zur Diskussion leistet ein Thesenpapier[6] der Arbeitsgruppe „Rechtsrahmen des Cloud Computing" innerhalb des Technologieprogramms Trusted Cloud[7] des Bundesministeriums für Wirtschaft und Energie. Auch hier wird das Thema Schweigepflicht bei der Auslagerung von IT-Dienstleistungen behandelt. Es werden die – aus Sicht dieser Gruppe – zu beseitigenden Schwierigkeiten geschildert, die bei der Auslagerung von IT-Dienstleitungen durch schweigepflichtige Berufsgruppen entstehen. Dieses Thesenpapier behandelt denkbare rechtliche Lösungsansätze. Im gesamten Thesenpapier entsteht allerdings im Grunde genommen der Eindruck, dass die Schweigepflicht ein Hindernis für moderne IT darstellt. Nicht thematisiert wurde jedoch in dem Thesenpapier, welche Gründe bei der Anwendung moderner IT für die Beibehaltung der Schweigepflicht sprechen. So entsteht, vielleicht unbeabsichtigt, der Eindruck, dass durch Cloud Computing die Schweigepflicht unnötig wird.

In diesem Artikel wird ein anderer gedanklicher Ansatz verfolgt. Er geht von der Notwendigkeit der Schweigepflicht als Schutz der Betroffenen aus.[8] Dies dürfte nachvollziehbar sein, da die Weiterentwicklung von Auswertungsmöglichkeiten und die immer weiter gehende Informationsvernetzung die Bedrohung der Rechte des Einzelnen eher vergrößern, als dass sie sie mindern.

Die Situation heute

Wie eingangs bereits erwähnt, ist Outsourcing heute in weiten Bereichen Realität. Die Formen des Outsourcings sind vielfältig und gehen von einer Wartung durch Techniker vor Ort über die klassische Datenverarbeitung im Auftrag bis zur Anwendung von Cloud Computing. Der Einsatz aller dieser Formen ist aber häufig mit einem strafrechtlichen Risiko für die Anwender verbunden.[9] Anders gesagt: In vielen Fällen könnte eine unbefugte Offenbarung der durch die Schweigepflicht geschützten Daten vorliegen.

Die Argumente für ein Outsourcing sind vielfältig. Sie reichen vom wirtschaftlichen Vorteil, über die Notwendigkeit des Einsatzes von Experten, bis zur Verbesserung der Sicherheit, die durch das Outsourcing erreicht werden soll.

Kostenvorteile durch Outsourcing?

Sehen wir von der prinzipiellen Frage ab, ob Kostenvorteile allein Verstöße gegen Strafgesetze rechtfertigen bzw. ob Kostenvorteile die gesetzliche Aufweichung eines prinzipiellen Schutzgedankens rechtfertigen können.

Ganz pragmatisch wäre zu prüfen, ob die Kosten bei einem Outsourcing wirklich geringer sind, als die Kosten für einen Eigenbetrieb. Bei diesem Kostenvergleich müssen aber auch Kosten für die Umstellung und einen möglichen Anbieterwechsel mit berücksichtigt werden. Die verantwortliche Stelle muss ja trotz des Outsourcings noch so viel Know-how vorhalten, dass ein Anbieterwechsel unproblematisch und kurzfristig möglich ist. Andernfalls würde sie sich dem Anbieter auf Gedeih und Verderb ausliefern. Hier ist außerdem sicher nach den unterschiedlichen Interessengruppen zu differenzieren.

Beim Blick auf Ärzte, Anwälte, Steuerberater und andere kleine und mittelständische Anwender ist folgender Gedanke zu berücksichtigen: Aufwändige und integrierte Komplettlösungen, die alle Spezifikationen von Datenschutz und -sicherheit erfüllen, könnten diese Anwender evtl. überfordern. Hier spielen hohe Implementationskosten und der ständige Nachbesserungsaufwand durch Updates eine Rolle. Ab einem gewissen Komplexitätsgrad sind diese Komplettlösungen für diese Anwender nicht mehr kalkulier- und steuerbar. Die mit diesen Produkten verbundenen Kostenvorteile für die freien Berufe wären daher ggf. nur für „die Großen" der jeweiligen Branchen zu erreichen, während die Mehrzahl der Anwender davon möglicherweise nicht einmal profitieren würde.

Ein anderes Problem ergibt sich beispielsweise im Bereich der Krankenhäuser. Hier haben die angebotenen Komplettlösungen einen Komplexitätsgrad erreicht, der einerseits den Anbietermarkt stark einengt und andererseits den Anwendern (Krankenhäusern) letztlich nur geringe Einwirkungsmöglichkeiten auf technische Entwicklungen erlaubt. Auch hier verlieren die Anwender unter Umständen ihre Souveränität im Umgang mit den eigenen Systemen.

Die Wahrheit in der Mitte

Ein gewisser Bedarf an externer IT-Expertise wird für viele Anwender sicher notwendig oder nützlich sein. Insofern kann ein Reformbedarf für die Schweigepflichtregelungen nicht geleugnet werden. Ob die Anwender ihrer Garantenstellung gerecht werden können, wenn sie für sich tendenziell unbeherrschbare Systeme anwenden, sollte aber ebenfalls hinterfragt werden. Dies gilt umso mehr, da die Anwender bei externen Systemen meist die drohenden Gefahren nicht einschätzen können. Diese reichen von kriminellen Angriffen bis hin zu möglicherweise befugten Zugriffen anderer Staaten. Gerade bei Cloud-Systemen kann der Anwender diese Risiken nicht vollständig beurteilen.

Hier müsste also differenziert werden zwischen einer vielleicht notwendigen Unterstützung mit Know-how und Angeboten, die selbst zahlreiche neue Risiken bergen. Insofern ist der von der Bundesanwaltskammer eingeführte Begriff der Sozialadäquanz durchaus sinnvoll. Jedoch gilt es ihn zu definieren, denn nur eine möglichst genaue Definition kann die Rechtssicherheit für beide Seiten (Anwender und ihre Klienten/Patienten oder Mandanten) sicherstellen. In der Diskussion um die Schweigepflicht werden zahlreiche Lösungsmöglichkeiten angeboten. Auf die Wichtigsten[10] wird hier kurz eingegangen. Da diese Lösungen isoliert den Schutz nicht vollständig gewährleisten, schwebt den Autoren eine geeignete Kombination dieser Ansätze vor. Allerdings scheidet nach ihrer Ansicht jede Lösung aus, bei der die Funktion der Schweigepflicht nicht mehr gewahrt oder technisch nicht umgesetzt werden kann.

1. Anpassungen von StGB und StPO
2. Bezugnahme auf datenschutzrechtliche Auftragsdatenverarbeitung
3. Erlaubnis in Berufsgesetzen, Anpassungen von StGB und StPO

1. Anpassungen von StGB und StPO

a. Zurzeit wird hier der Schutz durch die Schweigepflicht der betroffen Berufsgruppen und ihrer engen Mitarbeiter erreicht. Mit der Schweigepflicht korrespondieren das Recht zur Verweigerung der Aussage und der Schutz vor Beschlagnahme. Eine diskutierte Lösungsmöglichkeit wäre es die IT-Dienstleister in diese Gruppen aufzunehmen.

a. Die Anpassung des § 203 StGB. Problematisch dürfte hier die Erweiterung des Täterkreises sein. Die Mitarbeiter der IT-Dienstleister müssten wenigstens entsprechend geschult werden, da ihnen das Konstrukt der strafrechtlichen Schweigepflicht eher fremd sein wird. Außerdem ist zu klären, welche Verantwortung die Mitarbeiter des Dienstleisters haben, die an die Nutzung der bestehenden Systeme gebunden sind und dadurch evtl. schon bei der reinen Ausübung der Tätigkeit gegen die Schweigepflicht verstoßen müssen. Keinerlei Wirkung hätte eine Änderung des StGB für Dienstleister, die außerhalb Deutschlands tätig sind.

b. Die Anpassung der StPO. Für beide Fälle kennt die StPO bereits Sonderregelungen, zum einen nämlich den § 97 Abs. 2 Satz 2 StPO. Hier gibt es bereits Ausnahmen für den Gesundheitsbereich. Zum anderen wird der Kreis der Schweigepflichtigen im § 4f Abs. 4a BDSG um die betrieblichen Datenschutzbeauftragten der Geheimnisträger erweitert. In diesem Fall scheinen Erweiterungen also denkbar.

2. Bezugnahme auf datenschutzrechtliche Auftragsdatenverarbeitung

Dieser Ansatz soll durch eine strenge vertragliche Bindung der IT-Dienstleister den Schutz der Schweigepflicht herstellen.

Hier wäre vielleicht die Einfügung eines „§ 11a im BDSG zur Übermittlung an Dritte im Rahmen der Schweigepflicht" eine denkbare Lösung. Allerdings dürften in diesem Fall die Verträge, anders als im § 11 BDSG, nicht dem freien Spiel der Kräfte überlassen werden. Dies würde den Anbietern dieser Dienstleistungen zu viel Spielraum lassen. Vorstellbar wäre hier eine Lösung mit unveränderlichen Standardverträgen, die nicht nur technische Schutzmaßnahmen, sondern auch Haftungsfragen und strafrechtliche Verantwortung (s.o.) klären kann. Im § 203 StGB müsste dann festgestellt werden, dass eine Datenübermittlung im Rahmen des „11a BDSG" nicht unbefugt wäre. Zusätzlich wären natürlich die Anpassungen von StGB und StPO wie unter Nr. 1 dargestellt erforderlich.

3. Erlaubnis in Berufsgesetzen

Hier sollen die Berufsgruppen durch ihre eigenen Berufsordnungen befugt werden Daten zu offenbaren.

Jedoch könnte diese berufsspezifische Lösungen zu einer Zersplitterung der rechtlichen Regelungen führen. Als Ergänzung zu den beiden anderen Punkten, wäre eine Differenzierung nach Berufsgruppen aber durchaus hilfreich. Der Mandant eines Strafverteidigers braucht einen anderen Schutz als der Patient eines Arztes. Warum hier nicht sachgerechte Lösungen in der Berufsordnung definieren?

Fazit

Zusammenfassend lässt sich feststellen, dass sich je nach der Ausgestaltung des Outsourcings sehr unterschiedliche Beurteilungen ergeben.

Auftragsdatenverarbeitung und Fernwartung lassen sich regional begrenzen, die Verfahrensweisen dabei lassen sich regeln, so dass sich der Kreis derer, die in die Datenverarbeitung involviert sind, deutlich fassen lässt. Hier sind klare Strukturen möglich, die durch Aufsichtsbehörden geprüft werden können. Ebenfalls sind Regelungen zur Wahrung der Funktion der Schweigepflicht denkbar. Das Schutzziel der Schweigepflicht würde somit die technische Ausgestaltung der Verfahren weiterhin normieren.

Anders verhält es sich, wenn die Datenverarbeitung und der damit betraute Personenkreis die regionalen und nationalen Grenzen verlassen. Hier sind im Endeffekt Transparenz, Regelung oder gar Kontrolle nicht mehr möglich. Auch das nationale Recht lässt sich auf solche Strukturen nicht mehr anwenden und kann so keinen Schutz entfalten.

In der Cloud verliert der Auftraggeber letztlich prinzipiell immer seine Souveränität. In diesem Umfeld dürften sensible, schweigepflichtbewehrte Daten eigentlich nur qualifiziert inhaltsverschlüsselt abgelegt sein. Hier kann der Auftraggeber sonst seiner Garantenstellung nicht mehr gerecht werden. Solche Lösungen sind andernfalls nur unter Verzicht auf den Schutz der Schweigepflicht denkbar.

Eine Einbindung von IT Dienstleistungen, unter Wahrung des Schutzes der Schweigepflicht, ist zwar in regional und technisch begrenzter Form denkbar, aber beim Verlassen des nationalen Rahmens lässt sich dieser Schutz nicht aufrechterhalten. Gleiches gilt beim Einsatz komplexer Systeme, hier besteht die Gefahr, dass diese Systeme für den Anwender nicht beherrschbar sind.

1 Petri DuD 12/2014, S. 805

2 Besser bekannt ist hier vielleicht die Schreibweise Hiob

3 Ijob, 1,6-22, 2,1-10 zitiert nach Petri DuD 12/2014, S. 805

4 Zur Offenbarung „digitalisierter Geheimnisse" beispielsweise: Nomos-Kommentar-StGB Kargl § 203 Rn. 21

5 http://anwaltsblatt.anwaltverein.de/de/news/satzungsversammlung_11-2014

6 http://www.trusted-cloud.de/media/content/150129_Thesenpapier_Schweigepflicht_gesamt_RZ_Ansicht_EZ.pdf

7 http://www.trusted-cloud.de

8 Ähnlich, wenn auch in einem anderen Zusammenhang die Bundesbeauftragte für Datenschutz und Informationsfreiheit Andrea Voßhoff: *„Datenschutz ist kein „altes Vorrecht", das angesichts sich überschlagender technischer Entwicklungen und auf dem Altar technologischer Effizienz geopfert werden müsste."* Zitiert nach: Sonderveröffentlichung zu RDV 02/2015 S. 18.

9 Siehe Thesenpapier Schweigepflicht a.a.O. S. 10

10 Vergl. wiederum Thesenpapier Schweigepflicht a.a.O. S. 18f. Auf weitere Punkte z.B. die Konkretisierung des Offenbarungsbegriffes kann aus Platzgründen nicht eingegangen werden.

Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Flugzeugkatastrophe kein Grund zum Bruch des Patientengeheimnisses

Vor dem Hintergrund der Flugzeugkatastrophe in Südfrankreich am 24.03.2015 spekulieren die Medien, ob Co-Pilot Andreas Lubitz psychisch krank war und deshalb die Germanwings-Maschine 4U9525 abstürzen ließ. Lubitz war am Tag des Absturzes krankgeschrieben; das hatte er offenbar seinem Arbeitgeber verheimlicht. Außerdem wurde bekannt, dass Lubitz vor seiner Laufbahn als Pilot wegen suizidalen Neigungen in psychiatrischer Behandlung gewesen sein soll. Statt die Ermittlungen abzuwarten und dann zu untersuchen, ob und evtl. wie derartige Katastrophen in Zukunft verhindert werden können, hat eine unsägliche Debatte über gesetzgeberische Maßnahmen und über das Patientengeheimnis (ärztliche Schweigepflicht) begonnen.

- Politischer Aktionismus

Dirk Fischer, CDU-Abgeordneter im Bundestag, forderte: „Piloten müssen zu Ärzten gehen, die vom Arbeitgeber vorgegeben werden. Diese Ärzte müssen gegenüber dem Arbeitgeber und dem Luftfahrtbundesamt von der ärztlichen Schweigepflicht entbunden sein.“ Sein Fraktionskollege Thomas Jarzombek drängte auf eine Expertenkommission, die eine Richtschnur für Ärzte erarbeitet, nicht nur in Bezug auf Piloten, sondern auch auf Angehörige anderer Berufsgruppen, etwa Fernbusfahrer. Klaus Reinhardt, Vorsitzender des Hartmannbundes, plädierte dafür, die „Systematik von Krankschreibungen“ zu überdenken. Er halte es für überlegenswert, dass in speziellen Fällen der Arzt eine Krankschreibung ohne Angabe der Diagnose direkt an den Arbeitgeber leitet.

Das Standesrecht der Ärztekammern, das auf dem vor über 2000 Jahre festgehaltenen Eid des Hippokrates basiert, sieht vor: „Ärzte haben über das, was ihnen in ihrer Eigenschaft als Arzt anvertraut oder bekannt geworden ist, zu schweigen.“ Dazu gehören auch schriftliche Mitteilungen des Patienten, Aufzeichnungen über Patienten, Röntgenaufnahmen und sonstige Untersuchungsbefunde. Die Schweigepflicht gilt über den Tod des Patienten hinaus sowie gegenüber dessen Familienangehörigen. Ein Bruch des Patientengeheimnisses ist im § 203 des Strafgesetzbuches (StGB) verboten. Eine Entbindung von der Schweigepflicht ist auf der Grundlage eines Gesetzes oder durch die Einwilligung des Patienten möglich.

Auch wenn Ärzte nicht von ihrem Patienten von der Schweigepflicht entbunden wurden, dürfen sie in Ausnahmefällen nach § 34 StGB Auskunft geben, „soweit die Offenbarung zum Schutze eines höherwertigen Rechtsgutes vor schweren Schäden erforderlich ist“. Bei drohenden ganz gravierenden Straftaten kann sogar nach § 238 StGB eine Anzeigepflicht bestehen.

Der Präsident der Bundesärztekammer, Frank Ulrich Montgomery, wies darauf hin, dass die Entscheidung über den Bruch der Schweigepflicht nur „aufgrund der konkreten Umstände des Einzelfalls“ getroffen werden kann. Man könne aber davon ausgehen, dass das Interesse an der Abwehr konkreter Gefahren für Leib, Leben oder Gesundheit das Geheimhaltungsinteresse des Patienten überwiegt. In die Psyche eines Menschen kann tatsächlich nur begrenzt eingedrungen werden. Es gibt keine Sicherheiten gegen Amokläufe und gezielte Menschengefährdungen. Möglich sind gesundheitliche Vorsorgemaßnahmen; Tauglichkeitsuntersuchungen gibt es in vielen Berufen. Montgomery: „Kritische Reflexion ist immer sinnvoll. Wir haben aber eher Probleme mit einem zu laxen Umgang mit der Schweigepflicht“. Häufig würden Krankenhäuser nach dem Tod eines Menschen dessen Akten herausgeben, obwohl das verboten sei.

- Durchsuchungsbeschlüsse gegen Arztpraxen

Und genau auch das passierte im Fall Lubitz: Mehrere Arztpraxen im Raum Düsseldorf erhielten Besuch von den Fahndern der „Besonderen Aufbauorganisation Alpen“, die für die Düsseldorfer Staatsanwaltschaft unter dem Aktenzeichen 10 UJs 906/15 den Absturz untersucht. Die Fahnder legten jeweils einen Durchsuchungsbeschluss des Amtsgerichts Düsseldorf vor, mit dem die Ärzte vor die Alternative gestellt waren, entweder freiwillig die zu Lubitz geführten Akten herauszugeben oder das Archiv durchsucht zu bekommen. Trotz Skrupel übergaben die Ärzte die Unterlagen und setzten sich über ihre Schweigepflicht hinweg. Die Durchsuchungsbeschlüsse des Amtsgerichtes beriefen sich auf die Rechtsprechung des Bundesverfassungsgerichts, wonach „das öffentliche Interesse an vollständiger Wahrheitsermittlung“ im Zweifel auch die Beschlagnahme von Unterlagen rechtfertige, die von einer beruflichen Schweigepflicht geschützt werden. Dessen ungeachtet sind die Beschlüsse wahrscheinlich rechtswidrig, so wie dies auch Nikolaos Gazeas, Strafrechtsexperte an der Universität Köln sieht: „Das Amtsgericht hätte die Durchsuchungsbeschlüsse nicht erlassen dürfen. Was die Düsseldorfer Staatsanwälte tun, ist menschlich absolut nachvollziehbar, rechtlich jedoch absolut unzulässig.“ Da der Patient Lubitz tot ist, kann gegen ihn kein Ermittlungsverfahren mehr durchgeführt werden. Andere Beschuldigte gibt es nicht. Eine Zeit lang wurde ge-

prüft, ob sich ein Ermittlungsverfahren gegen Verantwortliche bei der Lufthansa oder der Tochter Germanwings einleiten lässt. Doch stellte die Staatsanwaltschaft keinen Anfangsverdacht fest. Zwar besteht auf die Staatsanwaltschaft ein „ungeheuer großer Erwartungsdruck“ durch die Öffentlichkeit. Staatsanwälte sind aber nicht eine investigative Abteilung für die Weltpresse. Die Staatsanwaltschaft rechtfertigte ihr Vorgehen mit Vorermittlungen in einem „Todesermittlungsverfahren“, da hier jemand eines nicht natürlichen Todes gestorben ist. Doch weshalb hierfür Durchsuchungsbeschlüsse bei dem Patientengeheimnis unterliegenden Ärzten erforderlich sind, erschließt sich nicht.

- Flugtauglichkeitsuntersuchung

Ein Arzt darf die zuständigen Behörden informieren, wenn ein Patient als Kraftfahrer am Straßenverkehr teilnimmt, obwohl er aufgrund einer Erkrankung (Alkoholsucht, Epilepsie) dabei sich und andere gefährdet. Es ist, so Montgomery, „jedoch erforderlich, dass der Arzt vorher ohne Erfolg auf den Patienten eingewirkt hat.“ Berufspiloten werden in Deutschland mindestens einmal pro Jahr auf ihre Flugtauglichkeit untersucht – von einem amtlich anerkannten Fliegerarzt. In anderen Ländern, etwa den USA, sei es üblich, die Ergebnisse direkt und personenbezogen der zuständigen Luftfahrtbehörde mitzuteilen, sagt Dirk-Matthias Rose, Leiter des Aeromedical Centers Flymed in Frankfurt am Main. Anders in Deutschland: Wird ein Pilot als nicht tauglich eingestuft, wird das Luftfahrtbundesamt (LBA) informiert und er dorthin verwiesen; das LBA kann eine Überprüfung verlangen.

Nach Ansicht des Deutschen Fliegerarztverbands müssen nicht hinsichtlich der Weitergabepflicht, sondern in Bezug auf die Untersuchungsqualität und -intensität Konsequenzen aus der Germanwings-Katastrophe gezogen werden, so Verbandspräsident Hans-Werner Teichmüller: „Wir fordern häufigere und gründlichere Laboruntersuchungen für Piloten.“ Es müsse ein Befund her, mit dem auch der Konsum von Psychopharmaka und Drogen nachgewiesen werden könne.

SPD-Gesundheitspolitiker Karl Lauterbach meinte, wenn Leib und Leben anderer Menschen gefährdet seien, sei „der Arzt verpflichtet, den Arbeitgeber über die Arbeitsunfähigkeit des Mitarbeiters zu informieren“. Dies trifft so nicht zu, wie Rose präzisiert: Im Zweifel – bei Fremd- oder Eigengefährdung – muss die Behörde verständigt werden: „Den Arbeitgeber selbst dürfen wir nicht informieren.“

Tatsächlich gibt das, was wir bisher über die Flugzeugkatastrophe wissen, keinen Anlass für eine Neuregelung der ärztlichen Schweigepflicht. Derartige populistische Forderungen sind reiner Aktionismus. Eine Lockerung des Patientengeheimnisses hätte den entgegengesetzten Effekt, nämlich eine größere Unsicherheit: Befürchtet ein Pilot, dass eine medizinische Diagnose umgehend an den Arbeitgeber weitergegeben wird, so wird er sich im Zweifel nicht Hilfe suchend an einen Arzt wenden. Die jüngsten Forderungen entspringen einem typischen Reflex in der politischen Arena: Der Ruf nach Gesetzesreformen ist nach Katastrophen programmiert. Bundesärztekammer-Präsident Montgomery erinnerte daran, dass die ärztliche Schweigepflicht ein „hohes Gut“ ist und nicht vorschnell wegen eines Einzelfalls aufs Spiel gesetzt werden darf (Siemens/Witte, Kranke Piloten: Das Wichtigste zur Debatte um die ärztliche Schweigepflicht, www.spiegel.de 30.03.2015; Strengere Regeln für Piloten, SZ 08.04.2015, 9; Darnstädt, „Absolut unzulässig“, Der Spiegel 16/2015, 28 f.).

Bund

Banken wollen mit Kundendaten Geld verdienen

Künftig wollen Banken in Deutschland Kundendaten genauer analysieren und damit Geld verdienen. Es geht dabei z. B. um die Analyse des Wohnortes und der Geschäftskontakte, die sich aus den Transaktionen ergeben. Bisher waren Ein- und Abbuchungen auf Girokonten über Einkäufe, Kredite, Versicherungen, Reisen und Shoppingvorlieben in Deutschland für andere als bankliche Zwecke tabu. Auf dieser Datengrundlage sollen KundInnen dann zugeschnittene Offerten aus dem Einzelhandel oder auch Empfehlung zu Versicherungs- und Energietarifen bekommen. Zwischen Commerzbank, Deutscher Bank, der ING-Diba und der HVB soll nach Presseberichten ein regelrechtes technologisches Wettrennen entbrannt sein, wer die ersten Datenanwendungen auf den Markt bringt.

Das Geschäft mit Vermittlungsprovisionen – das sog. Cross-Selling – soll dabei für die Banken nicht im Fokus stehen. Es soll vielmehr Zusatzangebote und Leistungen für die PrivatkundInnen geben, um Kontoführungsgebühren zu rechtfertigen. Bei der Direktbank ING-Diba arbeitet ein zwölfköpfiges Team an entsprechenden Anwendungen. Die Commerzbank hat neue Datenanwendungen schon jetzt bei ihrer polnischen Tochter MBank im Einsatz. Vorstand Markus Beumer freut sich, dass sein Haus über eine „immense Datenbasis – es grenzt nahezu an Big Data“ verfügt. Seine Bank wisse „viel mehr über unsere Kunden als Google oder Facebook“. Seit dem vergangenen Jahr bietet die Commerzbank hierzulande eine Smartphone-App für die mobile Kontostandsabfrage an.

Markus Pertlwieser, Chefentwickler für Digitales bei der Deutschen Bank erklärte: „Wenn der Kunde beispielsweise feststellt, dass er für eine Versicherung deutlich mehr ausgibt als der Vergleichsdurchschnitt, bekäme er von uns einen Hinweis auf günstigere Verträge.“ Es gehe nicht um Werbung und konkrete Produktempfehlung. Aber irgendwann, so hofft er, soll sich mit Ratschlägen und Anlagetipps Geld verdienen lassen, weil die Kunden bereit sind, für Dienstleistungen rund um ihr Konto Geld zu zahlen. Neben Zinsen, Provisionen und Krediten sollen Daten so zur vierten wichtigen Ertragsquelle werden. „Wir glauben, dass die Digitalisierung vor allem das Konto und die Verwendung von Daten revolutionieren wird“.

- Und der Datenschutz?

Bei der Deutschen Bank sind die Pläne so weit fortgeschritten, dass Vertreter des Instituts im Verbraucherschutzministerium vorstellig wurden. Gerd Billen, Staatssekretär im Bundesministerium der Justiz und für Verbraucherschutz, meinte dazu: „Wenn die Banken die Kontodaten ihrer Kunden für neue

Services verwenden, kann das durchaus im Interesse der Verbraucher sein, wenn alle rechtlichen Vorgaben eingehalten werden." Die für Banken besonders strengen Datenschutzbestimmungen und vor allem die kritische Öffentlichkeit setzen den Bemühungen enge Grenzen. Das Verbraucherschutzministerium nannte Bedingungen für entsprechende Datennutzungen: „Die Bank darf die Kundendaten weder verkaufen, noch sie anderen Interessenten zur Nutzung überlassen; das Einverständnis der Kunden muss vorliegen."

Für Dirk Vater von Bain & Company sind die deutschen KundInnen schwierige, beinahe gespaltene Persönlichkeiten. Einerseits erlaubten viele Menschen sozialen Netzwerken wie Facebook tiefe Einblicke in die Privatsphäre und das Konsumverhalten – andererseits sei man höchst kritisch gegenüber Banken. Bisher sei „es leichter für Banken, die Facebook-Daten der Kunden auszuwerten als die eigenen Daten der Kunden." Auch deshalb machen viele Banken aus ihren Plänen bislang ein großes Geheimnis. Bei der HVB verkleinert man derzeit das Filialnetz von 580 auf 340 Niederlassungen, investiert aber 300 Mio. Euro in mobile und internetbasierte Angebote. Wohin die Reise geht, machte Privatkundenvorstand Peter Buschbeck Anfang Februar 2015 deutlich: Banken würden künftig nicht nur als Berater, sondern als Sammler und Auswerter von Daten handeln: „Warum soll ein Kunde zukünftig mit einer Analyse seiner Ausgaben, etwa für Telekommunikation, Energieversorgung oder Versicherungen, nicht gleich auch entsprechende Vorschläge zu deren Optimierung von der Bank erhalten?"

Bei der Deutschen Bank fürchten sie, als Datenspion an den Pranger gestellt zu werden, der seine KundInnen auskundschaftet. Selbstverständlich stehe die Integrität der KundInnen über allem, versichert Markus Pertlwieser. „Wenn der Kunde das Gefühl hat, die Bank will ihm etwas verkaufen, wird er – vermutlich zu Recht – zögern. Es geht aber nicht zwingend um den Verkauf oder die Vermittlung von Produkten, sondern schlicht um eine für ihn wertvolle Information." In einem ersten Schritt plant die Deutsche Bank – im Gleichschritt mit anderen Instituten – Benachrichtigungsdienste für ihre Kunden. Jenseits der Visualisierung von Einnahmen, Ausgaben und deren Struktur können die Privat- und bald auch Geschäftskunden wohl der meisten Geldhäuser noch in diesem Jahr regelmäßige E-Mails oder SMS anfordern, wenn sie einen bestimmten Kontostand über- oder unterschritten haben oder eine wichtige Überweisung eingetroffen ist. Außerdem sollen sie Sparziele definieren und laufend kontrollieren können.

Sollten sich die Deutschen den neuen Angeboten dennoch verweigern, haben manche Institute auch schon einen Plan B in der Schublade. Wenn niemand die Auswertung seiner Daten erlaube, könnte das Konto auch als Tresor verkauft werden: für alle Daten und Dokumente, die der Kunde dort wegschließen möchte. Natürlich gegen eine ordentliche Gebühr – damit die Banken „endlich" wieder Geld verdienen.

- Die Praxis im Ausland

Im Ausland sind die Wettbewerber „weiter". Laut einer Studie von Capgemini glauben mehr als 90% der Finanzdienstleister in den USA, die Nutzung der Kundendaten werde darüber entscheiden, wer in der Branche noch eine Zukunft hat und wer nicht. Die Citigroup hat bereits spezielle Angebote entwickelt. So bietet sie Kreditkartenbesitzern in den USA an, die Preise aller mit der Karte bezahlten Produkte für zwei Monate zu beobachten. Sollte der Preis binnen 60 Tagen ab Kauf um 25 Dollar oder mehr sinken, erstattet die Bank die Differenz. In Chile versenden Millionen KundInnen der Großbank BBVA über Facebook Geld. In Polen erhalten 700.000 KundInnen der mBank auf Basis der Transaktionen auf ihren Konten sogar personalisierte Gutscheine und Rabatte, etwa für ihr Lieblingsrestaurant oder die beliebtesten Modemarken.

- Digitalisierung überall

Weit entfernt von den Frankfurter Glastürmen haben Programmierer damit angefangen, ganz neue und einfache Bezahlsysteme über das Netz oder das Smartphone zu entwickeln. Bill Gates meinte einst: „Banking is necessary, banks ar not". Die Banken erkennen generell bei der Digitalisierung Nachholbedarf, etwa auch im Bereich des mobilen Bezahlens, wo Unternehmen wie Apple längst eigene Bezahldienste anbieten. Facebook macht es inzwischen möglich, über das Netzwerk Geld zu versenden. Und Google betreibt einen eigenen Smartphone-Bezahldienst. Der Privatkundenvorstand einer großen deutschen Bank meinte: „Wir haben zehn Jahre komplett geschlafen und hatten Glück, dass dies kaum jemand bemerkt hat" (Banken wollen Kundendaten zu Geld machen, www.stern.de 09.03.2015; Schreiber/Kirchner Banken planen Datenanwendungen 17.03.2015; Schreiber/Kirchner, Banken wollen Daten ihrer Kunden zu Geld machen, www.capital.de 28.04.2015).

Bund

Kontodatenabfragen nehmen weiter zu

Deutsche Behörden haben 2014 bei der Suche nach SchuldnerInnen, Hartz-IV-Tricksenden und säumigen Steuerpflichtigen so oft wie noch nie zuvor private Kontodaten von BankkundInnen abgefragt. Gemäß einer Statistik des Bundesfinanzministeriums ließen neben den Finanzämtern insbesondere GerichtsvollzieherInnen prüfen, wer über welche Konten und Wertpapierdepots verfügt. Im Jahr 2014 zählte das Bundeszentralamt für Steuern (BZSt) mehr als 230.000 erledigte Kontenabrufe. 2013 waren es knapp 142.000 Abfragen. Das entspricht einem Anstieg von mehr als 60%. Im ersten Quartal 2015 verzeichnete das BZSt bereits 76.000 dieser Abrufe, was darauf hindeutet, dass sich im Jahr 2015 ihre Zahl weiter kräftig erhöhen wird.

Seit 2005 können Behörden Kontodaten abfragen, um z. B. SteuerschuldnerInnen oder schummelnden LeistungsempfängerInnen auf die Spur zu kommen. Den Kontostand oder einzelne Bewegungen auf dem Konto teilen die Kreditinstitute dabei nicht direkt mit. Anfrageberechtigt sind z. B. Steuerbehörden, die danach Pfändungen einleiten können, oder Jobcenter, wenn Hartz-IV-Empfänger nach Ansicht des Sachbearbeiters keine ausreichenden Angaben über ihre Vermögensverhältnisse vorlegen. Ebenso dürfen sich

Ämter, die Bafög, Wohngeld oder Sozialhilfe genehmigen, nach Namen, Geburtsdatum, Adresse und Kontonummer von BankkundInnen erkundigen.

Von den 230.000 Abfragen entfielen knapp 80 000 auf die Steuerbehörden, gut 10.000 mehr als 2013. Die anderen Ämter fragten in mehr als 150.000 Fällen die Daten ab – mehr als doppelt so viele wie im Vorjahr. Das Finanzministerium führt dies vor allem auf die 4.500 GerichtsvollzieherInnen zurück, die die Anzahl der Abrufe „deutlich erhöht“ hätten. Seit 2013 dürfen auch sie Auskünfte über SchuldnerInnen einholen. Detlef Hüermann, Bundesgeschäftsführer des Deutschen Gerichtsvollzieherbunds, erläuterte: „Es hat sich bei den Gläubigern herumgesprochen, dass es diese Möglichkeit gibt.“ Er meinte, dass dieses Instrument „fast nur bei nicht kooperativen Schuldnern genutzt wird, die keine Angaben zu ihrem Vermögen machen“. Erlaubt sei dies nur in bestimmten Fällen. Die Ansprüche des Gläubigers müssten sich u. a. auf mehr als 500 Euro belaufen. Komme dann heraus, dass ein Konto vorhanden ist, könne der Gläubiger eine Pfändung veranlassen.

Die Bundesdatenschutzbeauftragte Andrea Voßhoff sieht die Abfrageflut äußerst kritisch. In ihrem Tätigkeitsbericht heißt es: „Ursprünglich verfolgtes Ziel war die Austrocknung der Finanzströme des Terrorismus. Die nunmehr verfolgten Zwecke stehen hiermit in keiner Verbindung.“ Werden jedoch bereits bei der Kontoeröffnung die Stammdaten automatisch als Datensatz gespeichert und für die Abrufe verfügbar gemacht, „erfolgt letztlich eine anlasslose Erfassung grundsätzlich aller Kontoinhaber in Deutschland“ (Öchsner, Ämter forschen immer mehr private Konten aus, SZ 10.04.2015, 1; vgl. DANA 1/2014, 26, 2/2014, 76).

Bund

Presserat erweitert Online-Kodex

Der Deutsche Presserat hat die publizistischen Grundsätze im Hinblick auf onlinespezifische Anforderungen an die Presseethik ergänzt. Auf seiner Sitzung am 11.03.2015 in Berlin verabschiedete das Selbstkontrollgremium neue Richtlinien und aktualisierte bestehende Regelungen. Diese beruhen auf der Erkenntnis, dass das, was in der gedruckten Zeitung richtig ist, nicht für deren Online-Ausgabe gelten muss. Der Presserat stellt fest, dass die Presse die Verantwortung für Online-Beiträge trägt, die von Nutzenden zugeliefert werden. In der neuen Richtlinie 2.7 heißt es, dass solche Inhalte mit User-Generated-Content klar erkennbar sein müssen. Sollte in den Beiträgen gegen die Presseethik verstoßen werden, müssen diese von der Redaktion beseitigt werden, wenn sie davon Kenntnis erhält. Um solche Beiträge handelt es sich beispielsweise bei Nutzerkommentaren zu Online-Beiträgen.

Die neuen Richtlinien waren gemäß Presseratssprecher Tilmann Kruse notwendig geworden, da durch „spezifische Erscheinungs- und Veröffentlichungsformen in Online-Medien neue presseethische Fragestellungen aufgeworfen werden“. Eine weitere Änderung des Pressecodex betrifft die Veröffentlichung von Leserbriefen. Demnach ist es statthaft, dass unter Pseudonym veröffentlichte Online-Nutzerbeiträge, also insbesondere Kommentare von Nutzenden, auch als Leserbriefe in der gedruckten Ausgabe veröffentlicht werden können. Voraussetzung ist, dass auf die Quelle hingewiesen wird. Neuerungen gibt es zudem zum Thema Richtigstellungen. Demnach muss eine Richtigstellung bei einer Online-Veröffentlichung mit dem ursprünglichen Beitrag verbunden werden. Erfolgt sie in dem zugrunde liegenden Beitrag selbst, muss die Richtigstellung entsprechend gekennzeichnet werden. Im 1956 gegründeten Deutschen Presserat sind die Verlegerverbände BDZV und VDZ und die Journalistenorganisationen DJV und dju vertreten (Sagatz, Presserat erweitert Online-Kodex, www.tagesspiegel.de 12.03.2015; Presserat, Presserat stellt neue Online-Richtlinien vor, www.presserat.de 11.03.2015).

Bund

„Islamisten-Ausweis wirkt diskriminierend“

Der Passauer Rechtswissenschaftler Gerrit Hornung kritisierte am 16.03.2015 im Innenausschuss des Bundestags den von der Bundesregierung geplanten Ersatzpersonalausweis für Islamisten. Er habe Zweifel, ob die angestrebte Regelung mit dem Grundgesetz vereinbar sei: „Wenn durch das Dokument jeder sofort erkennen kann, dass der Inhaber als gewaltbereiter Islamist eingestuft wird, wäre das eine erhebliche Stigmatisierung. Dann wäre mit verfassungsrechtlich bedenklichen Diskriminierungen für die Betroffenen zu rechnen, angefangen beim Abholen eines Paketes bei der Post bis hin zum Abschluss eines Mietvertrags.“

Die Regierung will mit der Gesetzesänderung Islamisten die Ausreise in Kampfgebiete wie Syrien oder Irak erschweren. Ihnen soll künftig nicht nur der Reisepass, sondern auch der Personalausweis abgenommen werden können. Stattdessen sollen sie ein Ersatzdokument bekommen, um sich beispielsweise bei Banken oder der Wohnungssuche weiter ausweisen zu können. Auch die Bundesdatenschutzbeauftragte Andrea Voßhoff hatte bereits in einer Stellungnahme für den Innenausschuss vor „erheblichen Schwierigkeiten im Alltag“ für Inhaber des Ersatzausweises gewarnt. Die Voraussetzungen, unter denen ein solches Dokument ausgestellt wird, „müssten deswegen strikt auf die Personengruppe beschränkt bleiben, von der prognostisch eine entsprechende Gefahr ausgeht.“ Sie habe Zweifel, ob die Voraussetzungen streng genug formuliert sind (Zweifel an Islamisten-Ausweis, SZ 11.03.2015, 5; Gutachter kritisiert geplanten Islamisten-Personalausweis, www.spiegel.de 13.03.2015; Bedenken gegen Islamisten-Ausweis, der Spiegel 12/2015, 17).

Bund

Beim BfV massive Zunahme von stiller SMS

Das Bundesamt für Verfassungsschutz (BfV) hat im Jahr 2014 die Nutzung von „stiller SMS“ massiv ausgeweitet. Im zweiten Halbjahr 2014 versendete der deutsche Inlandsgeheimdienst 142.108 solcher heimlichen Nachrichten, mit denen über Anfragen bei den Mobilfunkbetreibern Mobilgeräte geortet werden können. Im ersten Halbjahr 2014 waren

es ca. 53.000. Im ersten Halbjahr 2013 lag der Wert noch bei 28.472. Zahlen zum Zoll wurden nicht öffentlich zur Verfügung gestellt. Die Verdreifachung der heimlichen Handyortung innerhalb eines halben Jahres beim BfV steht im Kontrast zum Bundeskriminalamt (BKA) und zur Bundespolizei (BPol), die derartige Aktivitäten zurückfuhren (BKA ca. 27.000, BPol ca. 39.000). Die Ausweitung steht offenbar in Zusammenhang mit der stetig wachsenden Zahl von Dschihadreisenden nach und aus Syrien und dem Irak.

Mit Hilfe von stiller SMS können Sicherheitsbehörden ein Mobilgerät bis auf wenige hundert Meter genau orten. Die Nachricht wird auf dem Display des Empfängers nicht angezeigt. Das Gerät bestätigt jedoch unbemerkt den Eingang der Nachricht. Die bei der Kommunikation anfallenden Verkehrsdaten werden dann von den Mobilfunkbetreibern beauskunftet (Geheimdienst setzt auf stille SMS, Der Spiegel 10/2015, 18, PE Linksfraktion im Bundestag, Der ausufernden Spitzelei des Verfassungsschutz mit „Stillen SMS“ Einhalt gebieten, 02.03.2015).

Bund

Generali konkretisiert deutsches Bonus-Projekt

Die private Generali-Krankenversicherung hat Einzelheiten zu den geplanten Anreizsystemen für gesundheitsbewusste KundInnen öffentlich gemacht. Der italienische Versicherungskonzern hatte im November 2014 eine viel beachtete Kooperation mit dem südafrikanischen Versicherer Discovery geschlossen (DANA 1/2015, 32 f.). Discovery hat unter dem Namen „Vitality“ ein Gesundheitsprogramm entwickelt, bei dem gesundheitsbewusste KundInnen Gutscheine und Prämienrabatte erhalten.

Ab Anfang 2016 sollen auch deutsche KundInnen der Generali ein sogenanntes „Vitality-Konto“ abschließen können und dann mit Boni und anderen Vergünstigungen für einen gesundheitsbewussten Lebensstil belohnt werden. Christoph Schmallenbach, Vorstand der Generali Deutschland, erläuterte vor der Presse in Köln: „Dabei kommt es nicht auf den vorhandenen Gesundheitszustand oder den Body-Mass-Index an.“ Entscheidend sei, wie sich der Versicherte künftig verhält. Um das zu messen, hat Discovery Vereinbarungen mit Unternehmen wie Nike, Fitbit und Garmin über die Nutzung von Wearables abgeschlossen. Das sind Armbänder oder andere Geräte, die Bewegung und sonstige gesundheitsrelevante Einflussfaktoren messen. Gemäß Schmallenbach finden außerdem Gespräche statt, wie die Angebote auf den deutschen Markt übertragen werden können. Geplant sind Kooperationen mit Supermärkten und Drogeriemarktketten, die bereit sind, in ihren Kassensystemen Produkte zu kennzeichnen, die für gesunde Ernährung stehen, etwa Obst oder Bioprodukte: „Rund 20 Prozent des Sortiments eines normalen Einzelhändlers fallen da rein.“ Die KundIn muss beim Kauf ihre Vitality-Karte vorlegen und bekommt dort Gesundheitspunkte gutgeschrieben. Punkte gibt es auch für Joggen oder andere Bewegungsformen, medizinische Vorsorge oder den Besuch von Fitnessstudios. „Das sind die drei Quellen: Ernährung, körperliche Aktivität und medizinische Vorsorge.“ Vitality vergibt je nach Verhalten der KundIn den Status Bronze, Silber oder Gold. Für Schmallenbach ist das Programm eine Gelegenheit, die Prävention zu stärken und den Kontakt zwischen Kundenschaft und Versicherung zu intensivieren: „Versicherung muss so erlebbar wie Facebook oder Amazon sein.“

Generali werde, so Schmallenbach, nur den Status zu sehen bekommen. Dafür gäbe es die entsprechenden Belohnungen, über die er aber noch keine Einzelheiten nannte. Es könnten Geschenke, aber auch Boni des Versicherers sein. „Wir werden uns da natürlich im Rahmen des deutschen Versicherungs-Tarifrechts und des Datenschutzes bewegen.“ Auch spezielle Tarifmodelle seien nicht ausgeschlossen. Schmallenbach: „Wir können damit ein Kollektiv identifizieren, das wir besser bepreisen können“. Der Konzern legt großen Wert auf digitale Zukunftsrojekte. Parallel findet ein internes Umbauprojekt mit dem Namen D2020 statt. Am 01.04.2015 übernahm der Generali-Manager Giovanni Liverani den Chefposten bei der Kölner Holding (Fromme/Hagen, Punkte sammeln, SZ 27.03.2015, 22; Generali konkretisiert Pläne, ftp.aerztezeitung.de 31.03.2015).

Baden-Württemberg

Offener Brief an den Verbraucherminister

von Thilo Weichert wegen der behördlichen Präsenz des Ministeriums auf Facebook (21.03.2015)

Sehr geehrter Herr Verbraucherminister Alexander Bonde,

„Alles was Spass macht, macht dick oder es verbieten einem die Grünen“. Diesen alten Spruch scheinen Sie widerlegen und auf den Datenschutz ummünzen zu wollen. Nur so kann ich Ihre öffentliche Kritik an Ihrem Landesbeauftragten für den Datenschutz Jörg Klingbeil verstehen, der Ihnen mit Schreiben vom 27.02.2014 mitteilte, dass er es als „ein ausgesprochenes Ärgernis“ ansieht, dass Ihr Haus auf Facebook ein Verbraucherportal eingerichtet hat.

Er verwies darauf, dass Facebook erst kürzlich verbraucherrechtswidrig neue Nutzungsbestimmungen und Datenschutzrichtlinien in Kraft gesetzt hat, weshalb der Bundesverband der Verbraucherzentralen (vzbv) erneut gegen dieses US-Internet-Unternehmen eine Unterlassungsklage erheben musste und die zuständige deutsche Datenschutzbehörde in Hamburg ein Verfahren einleitete. Nachdem Sie seiner Bitte, das „Verbraucherportal BW“ wieder abzuschalten, nicht nachkamen, wendete er sich – wie zuvor angekündigt – mit seinem Anliegen an die Öffentlichkeit. Hierauf reagierten Sie am 19.03. – ausdrücklich ausschließlich auf Facebook – mit Ihrem Post „Zurück zur Schreibmaschine löst das Datenschutzproblem nicht!“ Sie erklärten, Sie könnten die Aufforderung von Herrn Klingbeil „nicht nachvollziehen“: „Wie reflexhafte Boykott-Forderungen für soziale Netzwerke einen produktiven Anteil“ am Daten- und Verbraucherschutz haben sollen, sei Ihnen „schleierhaft“. Derartiges ignoriere „die Lebensrealität vieler Menschen“, der sich staatliche

Institutionen nicht entziehen könnten. Man müsse die Menschen gezielt dort informieren, „wo sie sich bewegen“, also u. a. bei Facebook. Ein „Hochtechnologieland wie Baden-Württemberg“ müsse auch im Netz eine starke Stimme haben. Auch Zeitungen und der SWR nutzten Facebook. Schließlich drehen Sie den Spieß gar um und fordern den Landesdatenschutzbeauftragten auf, Datenschutzrechte „auf allen Kanälen“, also auch über Facebook durchzusetzen: „Ein Zurück zur Schreibmaschine löst die Datenschutzprobleme nicht!“

Ich schreibe diesen „offenen Brief“ weniger in meiner Funktion als Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein und damit Kollege von Herrn Klingbeil, sondern weil ich mich in den 80er Jahren als grüner Landtagsabgeordneter und Politiker in Baden-Württemberg gegen die damals geplanten Volkszählungen engagierte und nicht glauben will, dass Ihre Haltung inzwischen die der Grünen „im Ländle“ ist.

Schon damals galt für uns nicht der in der alternativen Szene teilweise kursierende Spruch: „Legal, illegal, ...egal“. Der Verstoß gegen geltendes Recht durch die außerparlamentarische Opposition in der Form des zivilen Ungehorsams musste der Durchsetzung höherer Werte und Ziele dienen. Ein grünes Regierungsmitglied ist aber keine außerparlamentarische Opposition, sondern staatliche Gewalt, die gemäß Art. 20 Abs. 2 Grundgesetz an Gesetz und Recht gebunden ist. Das unterscheidet Ihr Ministerium von den Zeitungen, dem SWR und den über 20 Millionen Facebook-Nutzenden in Deutschland – bei aller begründeten Kritik an deren Facebook-Nutzung. Letztere handeln, wenn sie auf Facebook unterwegs sind, gar in Wahrnehmung ihres Rechts auf informationelle Selbstbestimmung.

Dass Facebook wesentlichste deutsche bzw. europäische Datenschutzregeln und viele Verbraucherschutzregeln verletzt, müsste Ihnen als Verbraucherminister bewusst sein. Der vzbv hat hierfür schon so manchen Nachweis erbracht. Viele europäische Datenschutzbehörden versuchen, der Datenschutzignoranz von Facebook etwas rechtsstaatlich entgegen zu setzen. Mir fällt tatsächlich kein internationales Internet-Unternehmen ein, das Verbraucherrechte derart nachhaltig und unverschämt ignoriert wie Facebook. Mit Ihrer behördlichen Präsenz bei Facebook stellen Sie sich als unentgeltlichen Kronzeugen für die Harmlosigkeit dieses Unternehmens zur Verfügung und schaffen damit eine Grundlage, dass dieses Unternehmen weiterhin erfolgreich sein illegales Geschäftsmodell verfolgt, das gekennzeichnet ist von Auskunfts- und Transparenzverweigerung, Verweigerung von Wahlmöglichkeiten für die Nutzenden, unzulässiger Klarnamenpflicht und Profilbildung... Herr Klingbeil wies Sie darauf hin, dass Facebook seine Werbeumsätze 2014 auf 11,5 Mrd. Dollar steigern konnte. Gar nicht zu sprechen von den demokratischen Gefahren, die von Facebook ausgehen. Sollten Sie insofern noch Informationsbedürfnisse haben, stehe ich gerne zur Verfügung.

Verbraucher- und Datenschutz sind ein zu ernstes Anliegen, um dabei launig zu argumentieren: Facebook ist nicht identisch mit dem Internet und allem Digitalen, es gibt noch andere Alternativen als die Schreibmaschine. Wahrscheinlich ist Ihnen der Unterschied zwischen einer behördlichen Warnung und einem Boykottaufruf bekannt. Ihnen muss klar sein, dass Facebook kein baden-württembergisches Unternehmen ist, sondern ein US-Konzern, der europäischen Startups das Leben schwer macht und sich durch Steuervermeidung hervortut. Vielleicht ist es Ihnen nicht bewusst: Mit Ihrer Argumentation replizieren Sie genau die Argumente des Weltkonzerns in den nunmehr schon über vier Jahren dauernden Auseinandersetzungen des ULDs mit Facebook. Sollte sich die „Lebensrealität“ dahin ändern, dass alle Welt nur noch den chinesischen Internet-Dienstleister Alibaba nutzt, so würden Sie auch dort Ihr Verbraucherportal einrichten?

Also, sehr geehrter Herr Minister: Überlegen Sie es sich doch bitte noch einmal.

Mit freundlichen Grüßen
Thilo Weichert

(Landesbeauftragter für den Datenschutz fordert Abschaltung der Facebook-Seite „VerbraucherBW“: „Ein Verbraucherportal auf Facebook ist ein Widerspruch in sich!“ https://www.datenschutz.de/news/detail/?nid=7134; Zurück zur Schreibmaschine löst das Datenschutzproblem nicht! https://www.facebook.com/VerbraucherBW/posts/760890710674982)

Berlin

degewo plant automatisches Schließsystem

Eine der größten Wohnungsgesellschaften in Deutschland, die Berliner degewo, will ihre mehr als 5.000 Mietshäuser mit einer neuen Schließtechnik ausrüsten. Die Türen der degewo-Objekte sollen künftig automatisch entriegelt werden, wenn sich BewohnerInnen, HausmeisterInnen oder die Müllabfuhr mit einem speziellen Chip in der Tasche räumlich nähern. Mit einem verschlüsselten Signal wird die Tür geöffnet. Dies soll eine Erleichterung für MieterInnen und Hausverwaltungen bringen. HandwerkerInnen, die regelmäßig im Haus arbeiten, sollen sich auch auf diese Weise Zugang verschaffen können. Die Technologie wurde von dem Berliner Start-up Kiwi.ki entwickelt. Auch die Deutsche Post und die Berliner Feuerwehr erproben das System (Der Spiegel 12/2015, 71).

Nordrhein-Westfalen

Polizeistudie mit Betroffenendaten im Netz

In einer im Internet veröffentlichten Studienarbeit wurden die vollen Namen mehrerer Opfer und Zeugen von Wohnungseinbrüchen in Düsseldorf genannt, die aus einer polizeilichen Datenbank stammen. Die Veröffentlichung zum „Predictive Policing“, also zur Prognose künftiger Straftaten und zu computergesteuerten Präventions- und Ermittlungsmethoden, war eine Abschlussarbeit an der Fachhochschule für öffentliche Verwaltung, wo Polizisten für den gehobenen Dienst ausgebildet werden. Sie war Anfang Februar 2015 auf dem Europäischen Polizeikongress in Berlin mit einem „Zukunftspreis“ ausgezeichnet worden. Als die Hochschule auf die Ver-

öffentlichung, die ohne das Wissen der Betroffenen erfolgt war, hingewiesen wurde, nahm sie diese sofort von ihrer Homepage: „Wir bedauern es sehr, dass die Daten zu diesen Sachverhalten so im Netz nachlesbar waren.“ In Zukunft werde man zusätzliche Sicherheitsmechanismen etablieren, um einen größtmöglichen Schutz für solche sensiblen Daten zu gewährleisten“ (Der Spiegel 11/2015, 20).

Thüringen

Verzicht auf Geheimdienst-V-Leute

Das Land Thüringen setzt eine Vereinbarung aus dem rot-rot-grünen Koalitionsvertrag um und schaltet sämtliche V-Leute beim Verfassungsschutz ab, auch „zum Zweck der Terrorismusbekämpfung“. SPD-Innenminister Holger Poppenhäger traf diese Entscheidung in Abstimmung mit Ministerpräsident Bodo Ramelow (Linke) und informierte hierüber die Parlamentarische Kontrollkommission des Landtages. Auf der Basis des Koalitionsvertrags werde das „System der V-Leute nicht fortgeführt.“ Poppenhäger und Ramelow haben sich über die Weiterbeschäftigung „einiger Quellen“ verständigt. Aus dem Umfeld des Verfassungsschutzes heißt es, es gebe zwar keine V-Leute mehr in der rechten Szene, beobachtet würden aber derart weiterhin die Salafisten oder die türkische PKK. Bis Ende 2015 sollen noch sogenannte Nachsorgetreffen abgehalten werden. CDU-Fraktionschef Mike Mohring kritisierte die Entscheidung: „Rot-Rot-Grün führt Thüringen in die Isolation.“ Es sei „gefährlich und lebensfremd“, den Verfassungsschutz seiner wichtigsten Quellen zu berauben. Der Linken-Abgeordnete Steffen Dittes erwiderte, die Erfahrung zeige, dass das V-Leute-System nicht die Sicherheit erhöhe, sondern die Demokratie gefährde.

Andere Bundesländer erwägen einen solch weit gehenden Schritt derzeit nicht. Innenminister Markus Ulbig (CDU) vom Freistaat Sachsen, der ähnlich wie Thüringen vom Skandalen und Machtmissbräuchen seines Geheimdienstes gebeutelt ist, meinte, dass das Land für die „sensiblen Beobachtungen eines guten Verfassungsschutzes“ auf „unmittelbare Einschätzungen und Eindrücke von Menschen angewiesen“ sei. Innenminister Reinhold Gall (SPD) erklärte für die grün-rote Regierung in Baden-Württemberg, der Einsatz von V-Leuten sei „unverzichtbar“. In bestimmten Fällen könne der Staat „ohne den Einsatz menschlicher Quellen unmöglich feststellen“, welche Gefahren drohten. Das SPD-geführte Innenministerium der rot-grünen Regierung in Nordrhein-Westfalen erklärte, der Einsatz von V-Leuten sei ein nachrichtendienstliches Mittel, das insbesondere zur Überwachung von Extremisten notwendig sei.

In seiner ersten Regierungserklärung bekräftigte der erste gerade zum Ministerpräsident gewählte Linkenpolitiker Ramelow, der jahrelang selbst Beobachtungsobjekt des Verfassungsschutzes war, den Plan einer umfassenden Verfassungsschutzreform. Die Abschaffung des V-Leute-Systems in seiner bisherigen Form sei eine Konsequenz aus den Verbrechen der rechten Terrorzelle NSU. Der Thüringer NSU-Untersuchungsausschuss habe eine „grundlegende Reform des Landesamtes für Verfassungsschutz angemahnt“. U. a. müsse die parlamentarische und öffentliche Kontrolle des Geheimdienstes verbessert werden.

Derweil machen die Innenminister der Union gegen die neuen V-Leute-Regeln von Thüringen mobil. Lorenz Caffier aus Mecklenburg-Vorpommern, Sprecher aller deutschen Unionsinnenminister, erklärte diese zu „einem großen Fehler“ und drohte Ramelow mit der Isolation innerhalb des Verbunds der Sicherheitsbehörden. Caffier beteuerte, der Einsatz von V-Leuten sei „absolut unverzichtbar“. Ramelow reagierte hierauf empört und verwies auf das Versagen der Sicherheitsbehörden bei der Aufklärung der NSU-Morde. Das Vertrauen zu den Thüringer V-Leuten sei parteiübergreifend verschwunden (Verfassungsschutz: Thüringen schafft sämtliche V-Leute ab, www.spiegel.de 20.03.2015; Krach um V-Leute, SZ 23.03.2015, 6; Ein paar V-Leute, Der Spiegel 15/2015, 19).

Datenschutznachrichten aus dem Ausland

Europa

EU-Richtlinie gegen Verwertung von Unternehmens-Leaks

Der Verband der Zeitschriftenverleger (VDZ) warnt vor einer geplanten EU-Richtlinie zum Schutz von Geschäftsgeheimnissen. Bislang dürfen JournalistInnen alle Informationen verwerten, die ihnen zugespielt werden, solange sie diese nicht illegal erworben haben. Künftig sollen Unternehmen eine Berichterstattung verhindern können, sofern diese auf internen Papieren beruht. Zulässig soll das Enthüllen von rechtswidrigem Verhalten sein. Christoph Fiedler, im VDZ zuständig für Europa- und Medienpolitik: „Es droht eine Richtlinie, die die investigative Berichterstattung über Unternehmen wesentlich beschränken könnte.“ Von Nachteil sei auch, dass über Fragen, die sich aus der Richtlinie ergeben, letztlich der Europäische Gerichtshof entscheiden werde und nicht das Bundesverfassungsgericht, das die Meinungsfreiheit traditionell höher halte (Der Spiegel 19/2015).

Frankreich

Premier Valls stellt Entwurf für Überwachungsgesetz vor

Zehn Wochen nach den blutigen Anschlägen von Paris stellte Frankreichs Premierminister Manuel Valls am 19.03.2015 persönlich einen umfangreichen Gesetzentwurf seiner Regierung vor, mit dem die nationalen Geheimdienste potenzielle Terroristen entdecken und mutmaßliche Gotteskrieger „in Echtzeit“ aufspüren sollen, u. a. mit Hilfe von Lauschangriff, Kameraüberwachung in Wohnungen sowie dem Ausspähen privater Computer ohne vorherige richterliche Genehmigung. Der sozialistische Premier berief sich dabei auch auf den am Vortag erfolgten Terroranschlag in Tunis: „Die Welt hat sich verändert. Nichts ist wie vorher.“ Anwaltsverbände, Amnesty International sowie die französische Datenschutzbehörde, die Commission Nationale de l´Informatique et des Libertés (CNIL), warnten vor Verletzungen der Grundrechte und der Privatsphäre der BürgerInnen. Die CNIL warnte vor „schweren Konsequenzen für den Schutz des Privatlebens“. Am 05.05.2015 billigte das Parlament das Gesetz mit breiter Mehrheit. Neben den meisten Sozialisten votierten auch die Mehrzahl der Abgeordneten der bürgerlichen Opposition (UMP) für das Gesetz. Wegen des Protestes zivilgesellschaftlicher Gruppen sowie der Einwände großer Internetfirmen waren zuletzt die Zweifel bei etlichen Abgeordneten an dem Projekt gewachsen. Neben den Grünen, einigen Kommunisten und den beiden Abgeordneten des Front National verweigerten auch prominente UMP-Politiker wie der potenzielle Präsidentschaftskandidat Bruno Le Maire ihre Zustimmung.

Das Gesetz ermächtigt die Dienste nicht nur zu einer verstärkten Bekämpfung des Terrorismus, sondern auch zu Eingriffen, sobald sie „wichtige außenpolitische Interessen“ oder „übergeordnete wirtschaftliche, industrielle oder wissenschaftliche Interessen“ der Nation bedroht wähnen. Auch die vorbeugende Bekämpfung der organisierten Kriminalität wird als Ziel benannt. Deshalb geißelte der Chef der Pariser Anwaltskammer Pierre-Olivier Sur den Entwurf als „Staatslüge“. Niemand stelle sich gegen eine gezielte Überwachung von Terrorverdächtigen, „aber dieser Text zielt auf viele andere Bereiche. Das gefährdet unsere Freiheit.“ Das Gesetz könne das Demonstrationsrecht oder die Entscheidungsfreiheit privater Unternehmer aushöhlen.

Künftig sollen Frankreichs Ermittelnde ohne richterliche Genehmigung Mikrofone und Kameras in privaten Räumen installieren oder Fahrzeuge mit Peilsendern versehen können. Das Abhören von Mobiltelefonen soll bei Gefährdung der nationalen Sicherheit oder bei Terrorverdacht ohne justizielle Kontrolle erlaubt sein. Umstritten ist, inwieweit Telefone von Freunden und Bekannten künftig belauscht werden dürfen. Der Entwurf erlaubt die „Entourage“ von Verdächtigen ins Visier zu nehmen. Behördenvertreter verweisen darauf, dass die Terroristen vom Januar 2015 sich über Mobilgeräte abgesprochen haben, die unter dem Namen ihrer Ehefrauen registriert waren. Zur digitalen Überwachung sollen die Dienste berechtigt werden, bei Internet-Providern Black Boxes zu installieren, um sämtliche Metadaten ihrer KundInnen (Absender, Empfänger, IP-Adressen ...) in Echtzeit an die staatlichen Dienste zu übermitteln. So sollen automatisch Nutzende angezeigt werden, die verdächtige Websites ansteuern oder deren Verhalten einem für Kriminelle „typischen Schema“ folgen. Die Regierung versicherte, die Daten würden nur anonym gesammelt; allenfalls bei Terrorgefahr verfolge man die Identität der Nutzenden. Gespeichert würden nur Informationen über „illegale Aktivitäten“. Den Geheimdiensten soll erlaubt werden, in den PCs von Verdächtigen Software zu installieren, die live die Tastatureingaben verfolgt. Damit will man Dschihadisten bei Internet-Chats auf die Schliche kommen. Der Einsatz von sog. IMSI-Catchern, die sämtliche Handy-Gespräche im Umfeld abfangen, soll legalisiert werden. Zwecks Kontrolle ist eine neue Behörde vorgesehen, eine aus Richtern, Abgeordneten und einem technischen Experten bestehende Kommission. Zudem bekämen Frankreichs BürgerInnen erstmals das Recht, gegen eine vermutete Überwachung Einspruch beim obersten Verwaltungsgericht der Republik Einspruch einzulegen.

Das neue Gesetz wird die Kontrolle der Auslands- wie der Inlandsspione einschränken. Diese Aufgabe soll eine Kommission aus MagistratInnen und ParlamentarierInnen wahrnehmen, die sämtliche vom Amt des Premierministers vorgelegten Anträge auf Personenüberwachung überprüfen dürfen, deren Meinung aber unverbindlich bleiben soll. Statt eines Vetos könnte das Gremium Beschwerde beim Staatsrat einlegen.

Premier Valls, vordem als Innenminister schon für Terrorismusbekämpfung zuständig, wies den Vorwurf zurück, er beschreite denselben Weg wie der damalige US-Präsident George W. Bush nach den Anschlägen vom 11.09.2001: „Dies ist kein Patriot Act à la francaise; dies ist keine Massenüberwachung.“ Die Verteidiger des Entwurfes argumentieren, die Reform schaffe weitgehend nur einen überfälligen Rechtsrahmen „für Dinge, die unsere Geheimdienste schon längst tun“. Bisher geschehe dies auf der Grundlage von Dekreten in einer juristischen „Grauzone“. Die insgesamt sechs französischen Geheimdienste, die mit mehr als 12.000 Mitarbeitenden über ein Jahresbudget von 1,2 Mrd. Euro verfügen, hatten für sich klarere und verbindlichere Regelungen eingefordert. Unmittelbar nach den Anschlägen vom Januar 2015 hatte Valls angekündigt, binnen drei Jahren 2.680 zusätzliche Anti-Terror-Kräfte zu rekrutieren, um v. a. die Überwachung von Verdächtigen im Inland zu verbessern. Angeblich müssten ca. 3.000 „potenziell gefährliche Personen“ dauerüberwacht werden. Die Überwachung der Brüder Said und Chérif Kouachi, die das Attentat auf die Satirezeitschrift Charlie Hebdo verübten, war vor den Anschlägen eingestellt worden.

Präsident Francois Hollande, überrascht vom wachsenden Widerstand gegen das Gesetz, versprach im April, er werde das Gesetz vom Verfassungsgericht prüfen lassen, noch bevor es in Kraft tritt, nachdem es vom Parlament beschlossen worden ist (Wernicke, Neue Waffen gegen den Terror, SZ 20.03.2015, 8; Wernicke, Liberté für Frankreichs Geheimdienste, SZ 06.05.2015, 7).

Frankreich

Ermittlungen gegen Bürgermeister wegen Muslim-Statistik

Mit Listen angeblich muslimischer SchülerInnen hat der Bürgermeister der nahe Montpellier gelegenen Stadt Béziers, Robert Ménard, in Frankreich für Empörung gesorgt und die Justiz auf den Plan gerufen. Gegen ihn wurden am 05.05.2015 nach Angaben der Staatsanwaltschaft Vorermittlungen eingeleitet. Ménard, der im Jahr 2014 mit Hilfe der rechtsextremen Front National (FN) zum Bürgermeister gewählt worden war, hatte zunächst eingeräumt, dass er Statistiken über die Religionszugehörigkeit von SchülerInnen anlegen lässt. In Béziers seien „64,6 Prozent der Schüler“ Muslime. Auf die Frage eines Internetnutzers, wie er zu dieser Zahl gelangt sei, erläuterte Ménard, „Schulklasse für Schulklasse“ würden die Vornamen der Kinder erhoben. „Ich weiß, dass ich dazu kein Recht habe. Aber – Pardon, dass ich das sage – die Vornamen geben Aufschluss über die Religion.“ Wer das Gegenteil behaupte, ignoriere das Offenkundige. Ménard wurde nicht wegen seiner ideologisch fragwürdigen Ansichten zur 1-1/2-stündigen Vernehmung der Kriminalpolizei in Montpellier einbestellt, sondern wegen des Verdachts „des Besitzes illegaler Daten ethnischen Ursprungs“.

Auch gegenüber dem Fernsehsender France 2 bestätigte der ehemalige Vorsitzende der Journalistenorganisation Reporters sans Frontières (Reporter ohne Grenzen), dass er sich für die Listen der Vornamen der Kinder bediene. Staatsanwalt Yvon Calvet teilte mit, dass Vorermittlungen wegen illegalen Sammelns von Daten nach ethnischen Kriterien eingeleitet worden sind. Ménards Äußerungen sorgten für Aufmerksamkeit bis zur höchsten Regierungsebene. Premierminister Manuel Valls rief zu zügigem Handeln auf. Eine Zählung muslimischer Kinder wäre illegal und würde dem säkularen Verständnis Frankreichs zuwiderlaufen. Auf dem Kurznachrichtendienst Twitter schrieb der sozialistische Premierminister: „Schande für den Bürgermeister. Die Republik macht keinerlei Unterscheidung bei ihren Kindern.“ Innenminister Bernard Cazeneuve betonte, eine solche Datensammlung sei gesetzlich verboten. „Kinder nach ihrer Religion in Listen einzutragen, bringt uns in die düstersten Stunden unserer Geschichte zurück.“ Bildungsministerin Najat Vallaud-Belkacem sprach von „illegalen“ und „antirepublikanischen“ Praktiken. Politiker der konservativen UMP geißelten den „Verstoß gegen den Geist der Republik“. Fast wortgleich äußerte sich Präsident Francois Hollande im fernen Riad. Sogar die Chefin der FN Marine Le Pen suchte Distanz: Sie lehne ethnische Statistiken als unfranzösisch ab.

Tatsächlich verbietet ein französisches Gesetz seit 1978 „ethnische Statistiken“. Die Erhebung oder Speicherung aller Daten, die Frankreichs Bürger „direkt oder indirekt nach rassischer oder ethnischer Herkunft“ zählen oder sie gemäß ihrer „politischen, philosophischen oder religiösen Überzeugungen“ sortieren, ist strafbar, maximal mit 300.000 Euro Geldbuße oder 5 Jahren Haft. Dies ist der Preis für einen Verstoß gegen das in Frankreich heilige Verbot der Gleichheit – der Egalité. Dieses Daten-Tabu führt dazu, dass die Schätzungen für die im Land lebenden Muslime von 2 bis 10 Millionen schwanken. Cran, eine Organisation schwarzer MitbürgerInnen, kritisiert dies als „Vogel-Strauß-Politik“: „Es ist, als würde ein Arzt sich weigern, ein Thermometer zu gebrauchen.“

Das Gesetz von 1978 lässt in Ausnahmen streng wissenschaftliche Fragen nach der Herkunft zu. Forschungsdirektor Patrick Simon vom Nationalen Institut für demografische Studien beklagt dennoch die Rechtslage, weil solchen Studien „ein Image der Illegitimität“ anhänge. Alain Jakubowicz, Präsident der Internationalen Liga gegen Rassismus und Antisemitismus, erkennt das Problem, findet das Tabu aber dennoch richtig: „Das ist die Folge, dass unsere Vision der Gesellschaft einem Traum folgt – und nicht der Wirklichkeit.“ Der Glaube an die eine gleiche Gemeinschaft gehöre zum Selbstverständnis der Republik. Ménard bestritt nach den ersten heftigen Reaktionen, Computerdateien über die Schüler angelegt zu haben. Wie er 64,6% kalkulierte, wolle er allenfalls dem Staatsanwalt verraten (Wernicke, Die Blindheit der Zahlen, SZ 07.05.2015, 7; Französische Stadt ließ muslimische Schüler zählen, www.welt.de 05.05.2015).

Großbritannien

IPT erklärt Rohdaten-Austausch zwischen NSA und GCHQ für bis vor kurzem illegal

Das britische Geheimdienst-Gericht Investigatory Powers Tribunal (IPT) entschied am 06.02.2015, dass der Zu-

griff des Government Communications Headquarters (GCHQ) auf Kommunikationsdaten von Millionen Menschen aus Datenbanken der NSA illegal war. Im Juli 2013, ein Monat nach den ersten Snowden-Enthüllungen, hatten u. a. die britische Bürgerrechtsorganisationen Privacy International und Liberty Klage eingelegt. Das ITP ist das einzige britische Gericht, das die Geheimdienste GCHQ, MI5 und MI6 beaufsichtigt. Damit hat das Gericht erstmals in seiner 15-jährigen Geschichte gegen diese Nachrichten- und Sicherheitsdienste geurteilt.

Gemäß der Entscheidung war der Zugriff auf Daten von PRISM und dem Glasfaser-Abhörprogramm Upstream bis Dezember 2014 unrechtmäßig, weil die Regeln für den Datenzugriff geheim waren. Während des Verfahrens hatte die britische Regierung diese Austausch-Regeln veröffentlicht. Weshalb der GCHQ inzwischen sich an die Gesetze halte, begründete das IPT nicht. Seitdem darf gemäß der Entscheidung legal geschnüffelt werden. Im äußerst knapp gehaltenen Urteil geht es um die Verarbeitung von Daten britischer Bürger und Bürger in Großbritannien, die von der NSA abgegriffen und nach Großbritannien weitergeleitet wurden. Damit sei gegen deren Recht auf Achtung des Privat- und Familienlebens verstoßen worden, wie es Artikel 8 der Europäischen Menschenrechtskonvention (EMRK) festschreibt. Über einen Ringtausch überwachen mehrere Geheimdienste immer nur Ausländer, geben diese Daten dann aber untereinander weiter. Dadurch werden Überwachungseinschränkungen oder -verbote für Inländer ausgehebelt.

Im Dezember 2014 hatte das regierungsunabhängige IPT noch andere Überwachungsmaßnahmen für legal erklärt. Seit Beginn der Snowden-Enthüllungen hatten Bürgerrechtsorganisationen wie Privacy International immer wieder Beschwerden eingereicht, wenn ein neues britisches Überwachungsprogramm ans Licht der Öffentlichkeit gelangte. Mit ihrem erfolgreichen Vorgehen gegen die GCHQ-Kooperation bei PRISM – Datenabgriff bei Internetdiensten wie Facebook – und Upstream – Datenabgriff direkt an Internetkabeln – erzielten sie nun ihre ersten Erfolge. Die klagenden Organisationen wollen nun erreichen, dass die vor Dezember 2014 illegal gesammelten Daten gelöscht werden. Zudem kündigten sie eine baldige Klage vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) an, um auch die weiterhin stattfindende Massenüberwachung über den Atlantik hinweg zu überprüfen.

Eric King, Deputy Director von Privacy International erläuterte: „Schon viel zu lange verhalten sich Geheimdienste wie GCHQ und NSA so, als würden sie über dem Gesetz stehen. Die Entscheidung des IPT bestätigt der Öffentlichkeit, was viele Menschen die ganze Zeit gesagt haben. Im letzten Jahrzehnt waren GCHQ und NSA in ein illegales Programm zum Austausch von Daten aus Massenüberwachungsmaßnahmen eingebunden, von dem Millionen von Menschen auf der ganzen Welt betroffen sind. Wir dürfen Geheimdiensten nicht erlauben, dass diese ihre Programme zur Massenüberwachung weiterhin durch die geheime Interpretation von geheimen Gesetzen rechtfertigen können.“ Die Hauruck-Entscheidung der Regierung, die zuvor geheime „Vereinbarungen“ öffentlich zu machen, sei ungenügend, um dieses massives Schlupfloch in den Gesetzen zu schließen: „Wir hoffen, dass der Europäische Gerichtshof ein Urteil zu Gunsten der Privatsphäre und gegen unkontrollierte Staatsmacht fällen wird.“ James Welch, Legal Director für Liberty, ergänzte: „Die Geheimdienste haben allerdings weiterhin die größtenteils unbeschränkte Befugnis, sich durch die private Kommunikation von Millionen Menschen zu wühlen – und der Gerichtshof glaubt, dass die beschränkten Sicherheitsmaßnahmen, die während den Gerichtsverfahren im letzten Jahr aufgedeckt wurden, eine angemessene Schutzmaßnahme für unsere Privatsphäre darstellen. Wir sehen das anders.“ Der grüne Bundestags-Abgeordnete Konstantin von Notz kommentierte die Konsequenzen für die deutsche Politik: „Für die bundesdeutschen Geheimdienste stellt sich nunmehr noch dringlicher die Frage, inwiefern die pauschale Entgegennahme von Daten von GCHQ und NSA ebenfalls illegal und verfassungswidrig ist. Die Bundesregierung muss hier umgehend Klarheit über das genaue Ausmaß der Kooperation und die Rechtsgrundlagen schaffen“ (Meister, Gerichtsentscheidung in Großbritannien: Rohdaten-Austausch zwischen NSA und GCHQ war bis vor einem Monat illegal (Update), netzpolitik.org 06.02.2015; NSA-Skandal: GCHQ-Überwachung britischer Bürger illegal, www.heise.de 06.02.2015).

Schweiz

Abschied vom Bankgeheimnis

Das steuerliche Bankgeheimnis hat in der Schweiz im grenzüberschreitenden Verhältnis weitgehend ausgedient. Nach und nach musste das Land akzeptieren, dass das Zeitalter des automatischen Austauschs von Informationen über Finanzkunden (AIA) vor der Türe steht. Im Jahr 2017 werden die Schweiz und die EU-Mitgliedsstaaten damit beginnen, Kontodaten zu erheben und von 2018 an auszutauschen. Am 18.03.2015 einigten sich die Unterhändler der Schweiz und der EU-Kommission in Brüssel auf ein entsprechendes Abkommen zum automatischen Informationsaustausch. EU-Staaten sollen jährlich die Namen, Adressen und Kontodaten von allen EU-BürgerInnen erhalten, die in der Schweiz ein Konto haben. Auf Schweizer Bankkonten lagert mehr ausländisches Geld als in irgend einem anderen Land, teilweise unversteuert. Schon seit Jahren machten deshalb zahlreiche EU-Staaten und die USA Druck auf Steuerflüchtlinge und Banken, Schwarzgelder offen zu legen.

Noch ungeklärt ist die Zukunft des steuerlichen Bankgeheimnisses innerhalb der Schweiz. Eine Rolle dabei spielt eine Volksinitiative zum Schutz der Privatsphäre (Matter-Initiative) sowie eine aktuelle Diskussion über den Teilumbau der Verrechnungssteuer in eine Zahlstellensteuer. Die Vernehmlassung (Anhörung im Rahmen der Gesetzgebung) zur Verrechnungssteuervorlage des schweizerischen Bundesrats lief Ende März 2015 ab. In diesem Paket ist vorgesehen, dass BankkundInnen künftig die Wahl zwischen Steuerabzug und Meldung an die Behörden haben sollen. KritikerInnen erwarten trotz des vorgesehenen Wahlrechtes, dass faktisch der

Druck in Richtung Meldeverfahren erhöht wird, das selbst in Wirtschaftskreisen kein Tabu mehr ist.

So hat sich der Wirtschaftsdachverband Economiesuisse in einer Vorstandssitzung positiv zu einem Meldeverfahren geäußert. Bevorzugt wird bei den Obligationenzinsen gar eine automatische Meldung an die Behörden ohne vorhergehendes Einverständnis der KundIn – vor allem weil mit dieser Variante ein relativ geringer administrativer Aufwand und geringe Haftungsrisiken verbunden seien. Der AIA wäre auch im Inland nicht eine völlige Neuheit. So kennt die Schweiz eine Art AIA mindestens zum Teil schon länger in Sachen Lohnausweise und bezüglich Zahlungsmeldungen von Versicherungen. Die Assekuranz muss Kapitalleistungen aus Lebensversicherungen sowie Leibrenten und Pensionen den Steuerbehörden melden, sofern die Betroffenen nicht Einspruch gegen die Meldung erhoben haben und die Alternative eines Verrechnungssteuerabzugs verlangen. In der Praxis wurden fast keine Einwände gegen solche Meldungen erhoben. Bei Dividendenerträgen soll es derweil laut Economiesuisse wie auch gemäß dem Vorschlag des Bundesrats bei der derzeitigen Verrechnungssteuer bleiben. Auch bei den Zinserträgen auf Bankkonten will Economiesuisse die Verrechnungssteuer beibehalten.

Enthalten haben sich bei der Vorstandssitzung die Vertretungen des Bankensektors, welcher von der Vorlage besonders stark betroffen ist. Die Bankiervereinigung hat noch keine klare Position bezogen. Eine Gruppe von inlandorientierten Banken (Raiffeisen, Migros-Bank, Kantonalbankenverband und Regionalbanken) hatte jedoch Anfang 2015 angedeutet, dass sie die Verrechnungssteuer gleich ganz abschaffen und dafür den AIA auch im Inland forcieren will. Haupttreiber dieser Haltung war der Wunsch, zwecks Reduktion der Verwaltungskosten auf den Zwang zu zwei parallelen Verfahren (Steuerabzug und Meldung) zu verzichten und zudem Haftungsrisiken wegen möglicher Fehler bei den Steuerabzügen zu vermeiden. Die Bankiervereinigung hat in dieser Frage bei Economiesuisse faktisch eine Art Vetorecht. Der erwähnte Beschluss des Wirtschaftsdachverbands steht unter dem Vorbehalt, dass die Bankiervereinigung zustimmt. Sollte sie das nicht tun, würde Economiesuisse dem Vorschlag des Bundesrats folgen, aber eine Aufwandentschädigung zugunsten der Banken für die Vornahme von Steuerabzügen sowie eine Reduktion der Haftungsrisiken fordern (Abschied vom Bankgeheimnis, SZ 20.03.2015; Schöchli, Abschied vom Tabu des Bankgeheimnisses, www.nzz.ch 19.3.2015).

USA

Hacker im Weißen Haus

Hackern ist es offenbar im Herbst 2014 gelungen, in ein Computernetzwerk des Weißen Hauses einzudringen. In einem Netzwerk des US-Präsidialamtes, das Mitarbeitende von Präsident Barack Obama nutzen, seien Besorgnis erregende Aktionen beobachtet worden, so Regierungsvertreter. Das Weiße Haus habe umgehend Gegenmaßnahmen eingeleitet. Der Zugang zu einigen Diensten des Netzwerks sei daher unterbrochen worden. Einige Angestellte hätten in der Folge mit vorübergehenden Systemausfällen und Verbindungsproblemen zu kämpfen gehabt. Die Regierungsvertreter versicherten, dass lediglich einige „Elemente des nicht vertraulichen Netzwerks betroffen“ gewesen seien. Systeme mit geheimen Informationen würden in einem getrennten Netzwerk betrieben. Die Hacker hätten aber Zugang zu nicht öffentlichen Informationen wie Details zum Terminplan von Präsident Barack Obama gehabt. Derartige Informationen seien für ausländische Geheimdienste wertvoll. Insgesamt habe die „Heftigkeit“ der Aktionen die US-Offiziellen überrascht.

Unklar ist, wer hinter der Cyberattacke steckt. Es wurde der Verdacht geäußert, dass die verantwortlichen Hacker für die russische Regierung arbeiten. FBI, Secret Service sowie der Geheimdienst NSA sind demzufolge an den Ermittlungen beteiligt. Der Hinweis, der zur Entdeckung des Angriffs auf das Netzwerk führte, soll von einem Verbündeten gekommen sein. Das Büro des US-Präsidenten sowie anderer Regierungsstellen und Ministerien geraten immer wieder ins Visier von Hackern. Obamas Büro erreichten täglich Warnungen zur Cyberspionage, sagte ein Regierungsbeamter.

Russland wies die Berichte entschieden zurück. Kremlsprecher Dmitri Peskow erklärte am 08.04.2015 in Moskau: „Das ist inzwischen schon zum Sport geworden: Für alles wird Russland verantwortlich gemacht. Hauptsache, niemand findet demnächst im Fluss Potomac russische U-Boote, wie das schon in anderen Ländern der Fall war.“ Russland sei an einer Zusammenarbeit mit den USA bei der Lösung internationaler Krisen und Probleme interessiert. Eine gegenseitige „Dämonisierung“ lehne Moskau ab.

Der Hackerangriff war, so Presseberichte, eine der ausgeklügeltsten Cyberattacken, die jemals gegen das Weiße Haus ausgeführt worden seien. Die Hacker hätten ein E-Mail-Konto des US-Außenministeriums als Ausgangspunkt benutzt, um in das Netzwerk des Weißen Hauses einzusteigen. Dabei setzten die Hacker auf das sogenannte „Spear Phishing“. Das beschreibt personalisierte und gezielte Bemühungen, von Mitarbeitenden Passwörter und andere Zugangsinformationen abzufangen. Dazu werden z. B. E-Mails verschickt, die aussehen, als kämen sie von der eigenen IT-Abteilung (Russische Hacker im Weißen Haus? www.mainpost.de 08.04.2015; Horchler, Zielscheibe Obama – Hacker im Weißen Haus, www.tagesschau.de 29.10.2014).

USA

Mit Wirtschaftssanktionen gegen Hacker

Im Kampf gegen Cyberangriffe setzen die USA nun auch auf Wirtschaftssanktionen. Eine am 01.04.2015 von US-Präsident Obama unterzeichnete Anordnung ermöglicht es, das Vermögen von Hackern einzufrieren. Dies sei wegen der Zunahme von „bösartigen Cyberaktivitäten“ notwendig. Obama rief angesichts der Zunahme von „bösartigen Cyberaktivitäten“ gegen die USA einen nationalen Notstand aus. Die Sanktionsliste wird den Angaben zufolge gemeinsam vom Finanz-, Außen- und Justizministerium in Washington erstellt. Die

Strafmaßnahmen sollen unter anderem bei Attacken auf wichtige Infrastruktur wie die Strom- oder Wasserversorgung, beim Diebstahl von Bank- und Kreditkarteninformationen sowie bei der Entwendung von Industriegeheimnissen greifen.

Obama drohte sowohl einzelnen Hackern als auch Unternehmen, die von den Cyberangriffen profitieren, mit Konsequenzen. Ausdrücklich erwähnte der Präsident Attacken aus China, Russland, Nordkorea und dem Iran. Bislang sei es wegen schwacher Gesetze und dem Unwillen ausländischer Regierungen oftmals schwierig gewesen, „schlechte Akteure“ zur Rechenschaft zu ziehen. Als Reaktion auf eine Welle von Hackerattacken hatte Obama bereits im Januar 2015 schärfere Gesetze zur Cybersicherheit angekündigt. Mutmaßlich nordkoreanische Hacker hatten im vorangegangenen November die Computersysteme des Filmstudios Sony Pictures geknackt und anschließend vertrauliche Informationen im Internet veröffentlicht. Mit dem Datenleck wollten sie die Absetzung der Politkomödie „The Interview“ erzwingen, die von einem fiktiven Mordkomplott gegen den nordkoreanischen Machthaber Kim Jong Un handelt. Die Führung in Pjöngjang wies jede Verantwortung zurück.

Millionen von Verbrauchern in den USA wurden in den vergangenen Jahren Opfer von Datendiebstahl durch ausländische Hacker. Alleine durch eine Cyberattacke auf den Einzelhandelsriesen Target sollen die Kreditkarteninformationen von bis zu 40 Millionen Kunden in die Hände von Kriminellen gelangt sein. China steht im Verdacht, eine Sondereinheit seiner Volksbefreiungsarmee einzusetzen, um Handelsgeheimnisse von US-Unternehmen zu stehlen (Mit Sanktionen gegen Hacker www.tagesschau.de 01.04.2015).

USA

JP Morgan will Mitarbeiter-Fehlverhalten per Algorithmus feststellen

Die US-Investmentbank JP Morgan Chase will einen Algorithmus nutzen, um Fehlverhalten von Mitarbeitenden auf die Schliche zu kommen. Sie sammelt von diesen unterschiedlichste Arten von Daten und analysiert diese, um zweifelhaftes Verhalten in einer Art Frühwarnsystem aufzudecken. Im Idealfall sollen gegen Regeln verstoßende Mitarbeitende identifiziert werden, bevor sie der Bank oder KundInnen schaden können. Analysiert werden u. a. Angaben, ob ein Börsenhändler bestimmte Risikogrenzen überreizt, ob er gegen Handelsregeln verstößt oder ein Seminar über Verhaltensregeln schwänzt. Der Algorithmus kombiniert diese Daten und schlägt Alarm, wenn sich aus dem Verhalten eines Mitarbeitenden ein bestimmtes Muster ergibt.

Amerikanische und europäische Großbanken waren in den vergangenen Jahren in zahlreiche Skandale verwickelt. Sie manipulierten Zinsen und Währungen zu ihren eigenen Gunsten, zogen Kunden mit minderwertigen US-Immobilienkrediten über den Tisch und etliche Male verzockten Händler auch das Geld der eigenen Bank. JP Morgan, Amerikas größte Investmentbank, war bei vielen dieser illegalen Praktiken dabei. Die Kosten für Rechtsstreitigkeiten beliefen sich in den letzten Jahren auf ca. 36 Milliarden Dollar (33,5 Milliarden Euro). JP-Morgan-Chef Jamie Dimon, mit 20 Millionen Dollar Einkommen im Jahr 2014 einer der bestbezahlten Banker der Wall Street, will mit dem Verfahren Verhaltensprognosen anstellen, mit denen Schaden von der eigenen Bank abgewehrt wird.

Sally Dewar, Leiterin der Rechtsabteilung von JP Morgan in Europa, meinte: „Es ist sehr schwierig für einen Vorgesetzten, aus Hunderten von Daten bestimmte Themen zu erkennen, die sich für einen Händlertisch ergeben.“ Die Idee sei es, anhand der Daten Vorhersagen über bestimmte Verhaltensmuster zu treffen. Das Softwareprogramm wurde bereits in den Handelsräumen von JP Morgan getestet. Von 2016 an soll es auch in den Investmentbanking-Bereichen und in der Vermögensverwaltung angewandt werden. Das Experiment ist auch für andere Investmentbanken interessant. Viele, z. B. auch die Deutsche Bank, wollen ihre Mitarbeitenden zu einem Kulturwandel anstiften. Das Wissen um die Algorithmen-Überwachung soll sie von zweifelhaftem Verhalten von vorneherein abhalten.

JP Morgan reagiert damit auch auf die Kritik, Großbanken täten zu wenig, um Missbrauch und Betrug zu verhindern. In der US-Politik wurde damit gedroht, das Investmentbanking künftig noch stärker vom Privatkundengeschäft zu trennen – so wie dies früher der Fall war. JP Morgan hat in den vergangenen drei Jahren 2.500 Mitarbeitende eingestellt, die sich ausschließlich um die Einhaltung von Verhaltensregeln kümmern. Die Bank hat zudem 730 Millionen Dollar ausgegeben, um die Prozesse zu verbessern. Stellenausschreibungen von JP Morgan zeigen, dass die Bank vermehrt Mitarbeitende sucht, die sich mit moderner Kommunikation per Internet und Smartphone auskennen. Dabei geht es wohl auch darum, E-Mails, Chats und Telefonate zu überwachen. Zum Zweck der Terrorismus-Bekämpfung werden schon heute E-Mails und Anrufe auf bestimmte Wörter hin untersucht.

Der E-Mail-Verkehr von Großbanken war ein wichtiges Beweismittel im Skandal um manipulierte Zinssätze wie dem Libor. Dabei verabredeten sich Händler einzelner Banken, die für die Feststellung des Zinses zuständig waren, diesen in eine bestimmte Richtung zu manipulieren, von der die Bank dann profitierte. Die Aufsichtsbehörden haben mehrere Banken, auch JP Morgen, deswegen zu Milliarden-Strafen verurteilt. JP Morgen war in die Manipulation von Devisenkursen verwickelt. Ihr Händler Bruno Iksil, genannt „der Wal von London“, verzockte mit riskanten Wetten auf Derivate in London allein 6,2 Milliarden Dollar.

Die Überwachung von Mitarbeitenden mit solchen Mitteln wirft eine Reihe von Datenschutzfragen auf: Kann man jemanden für etwas zur Rechenschaft ziehen, das er noch gar nicht getan hat? Wie ist die Computerkontrolle mit der persönlichen Handlungsfreiheit der Betroffenen vereinbar? Welche Informationen und Rechtsschutzmöglichkeiten haben Betroffene? Die JP-Morgan-Verantwortliche Dewar behauptete, man werde beim Sammeln der Daten vorsichtig vorgehen. Die Bank wollte nicht detailliert dazu Stellung nehmen, welche Daten sie genau erhebt und in welchen Bereichen ihre Mitarbeitenden auf welche Weise überwacht werden.

Im Februar 2015 schaltete JP Morgen zudem einen E-Mail-Account frei, in dem Mitarbeitende anonym Verdächtiges melden können. Der Organisations-Chef ermahnte Angestellte, die Verhaltensregeln einzuhalten und erinnerte daran, dass Skandale Boni für jeden mindern. 300 Führungskräfte bekamen ein Sondertraining, um besonders gefährdete Bereiche zu identifizieren. Dewar gibt jedoch zu, dass sich Betrug niemals ganz ausschließen lässt: „Wir haben nun größeres Vertrauen in Früherkennung. Aber ich denke, es wird niemals 100-prozentige Sicherheit geben."

In Deutschland werden bei Banken (noch) keine Algorithmen eingesetzt, um ein mögliches Fehlverhalten von Mitarbeitenden auszukundschaften. Institute, Wertpapierhäuser und Börsen haben jedoch eine Reihe Vorsichtsmaßnahmen getroffen, um folgenschwere Fehler und Betrug zu vermeiden. Eine davon ist das Vier-Augen-Prinzip: Wichtige Handelsgeschäfte darf niemals eine einzelne MitarbeiterIn abschließen; es gibt eine zweite Person, die darüber schauen muss. Große Betrugsfälle in der Vergangenheit, etwa der Fall Nick Leeson oder der Fall Jerôme Kerviel bei der Société Générale, haben gezeigt, dass der Missbrauch oft klein anfängt und die Händler dann immer größere Summen einsetzen müssen, um den Verlust zu verdecken – bis das Lügengebäude zusammenbricht. Aus diesem Grund sind Betrügende auch permanent in der Bank und können keinen Tag frei machen. Um dies zu vermeiden, ist bei einer deutschen Großbank ein mindestens zweiwöchiger Urlaub am Stück im Jahr vorgeschrieben. In dieser Zeit hat der Händler keinen Zugang zum System: „Das Wichtigste jedoch ist die Kultur. Man muss den Mitarbeitern schon bei der Einstellung sagen, dass sie hier falsch sind, wenn sie zocken wollen." Auch die Deutsche Börse trifft Vorkehrungen. So gibt es einen Sicherheitsmechanismus, damit sich bei der Eingabe einer Order niemand vertippt. Mancher Kurseinbruch bei einer Aktie ist in der Vergangenheit schon dadurch ausgelöst worden, dass beim Auftrag eine Kommastelle verrutscht war – das Problem des „fetten Fingers". An der Deutschen Börse wird zudem der Handel einer Aktie ausgesetzt, wenn sich der Kurs abrupt außergewöhnlich verändert (Freiberger, Der gläserne Händler, SZ 10.04.2015, 18).

Kanada

Parlament billigt weit gehendes Geheimdienstgesetz

Das Unterhaus des kanadischen Parlaments hat am 06.05.2015 mit 183 Abgeordenten gegen 96, also mit großer Mehrheit, einem umstrittenen neuen Anti-Terror-Gesetz zugestimmt, das die Befugnisse des nationalen Geheimdienstes erheblich ausweitet. Premierminister Stephen Harper verfügt dort wie auch im zustimmungspflichtigen Senat über eine komfortable Mehrheit. Die Regierung hatte das neue Anti-Terror-Gesetz Ende 2014 angekündigt, nachdem im Oktober bei zwei islamistischen Angriffen zwei Soldaten getötet worden waren. Einer der Angreifer war zudem ins Parlament eingedrungen, wo ihn Sicherheitskräfte erschossen. Kanadas Minister für öffentliche Sicherheit, Steven Blanley, erklärte im Parlament, mit dem neuen Gesetz solle verhindert werden, „dass die Terroristen des internationalen Dschihadismus, die uns bedrohen, zur Tat schreiten".

Das neue Gesetz weitet die Befugnisse des Geheimdienstes CSIS massiv aus. Bisher beschränken sich die Aufgaben des CSIS auf das Überwachen und Sammeln von Informationen. Um Terrorangriffe zu verhindern, soll er nun auch selbst aktiv werden dürfen – erstmals auch im Ausland. Das Gesetz ermächtigt den Geheimdienst, gegen Verdächtige vorzugehen, die sich dschihadistischen Gruppen im Ausland anschließen wollen. Dazu soll der CSIS künftig etwa den Onlinekauf von Flugtickets blockieren und verdächtige Finanztransaktionen stoppen können. Um Terrorangriffe zu verhindern, sind künftig auch Maßnahmen wie Abhöraktionen erlaubt, wenn ein Verdacht besteht. Um Festnahmen zu erleichtern, sollen die Fälle künftig in Geheimanhörungen einem Richter vorgelegt werden können. Ein Anwalt, der die Interessen des Betroffenen vertritt, ist nicht vorgesehen.

Der Gesetzentwurf löste in Kanada massive Proteste aus, u. a. von vier ehemaligen Premierministern, mehreren ranghohen Richtern, dem kanadischen Datenschutzbeauftragten und der Schriftstellerin Margaret Atwood. Umfragen zufolge lehnen auch mehr als die Hälfte der KanadierInnen das Gesetz ab. Die KritikerInnen monieren, das Gesetz verleihe den Geheimdiensten zu viel Macht und führe zu einer systematischen Überwachung des Internets. Die oppositionellen Sozialdemokraten von der Neuen Demokratischen Partei (NDP) sprachen von einem „verhängnisvollen" Gesetz. Deren Abgeordneter Randall Garrison wies darauf hin, dass tausende Menschen gegen die Pläne demonstriert haben, „die unsere Rechte und Freiheiten aushöhlen werden. Diese Leute wollen nicht, dass die Angst über die Werte unserer Demokratie triumphiert" (Kanadas Unterhaus für umstrittenes Anti-Terror-Gesetz, de.nachrichten.yahoo.com 07.05.2015).

Australien

Datenpanne beim G-20-Gipfel

Die australische Einwanderungsbehörde hat versehentlich persönliche Daten von TeilnehmerInnen des G-20-Gipfels an einen Fußballveranstalter verschickt. Gemäß Presseberichten waren von der Datenpanne insgesamt 31 Staats- und Regierungschefs betroffen, darunter Bundeskanzlerin Angela Merkel (CDU) und US-Präsident Barack Obama. Bei den versehentlich weitergeleiteten Informationen handelt es sich demnach unter anderem um die Passnummern und Angaben zum Einreisevisum für Australien. Ein Beamter der Einwanderungsbehörde habe die Daten Anfang November 2014 versehentlich per E-Mail an ein Mitglied des Organisationskomitees für die Fußball-Asienmeisterschaft gesendet, die im Januar 2015 in Australien stattfand.

Neben Merkel und Obama hatten auch der russische Präsident Wladimir Putin, der britische Premierminister David Cameron und der chinesische Präsident Li Xinping am G-20-Gipfel in Brisbane Mitte November 2014 teilgenommen.

Die australische Einwanderungsbehörde bestätigte die Datenpanne, wollte sich aber nicht zu Einzelheiten äußern. Die Daten seien, so eine Sprecherin, vom Empfänger sofort wieder gelöscht und nicht weiterverbreitet worden. Außerdem sei umgehend der australische Datenschutzbeauftragte informiert worden. Sie sagte nicht, ob auch die betroffenen Staats- und Regierungschefs informiert wurden (Passnummer von Kanzlerin Merkel per Mail verschickt, www.bild.de 30.01.2015).

Venezuela

Mit Fingerabdruckscanner in Supermärkten gegen den Schwarzmarkt

Die Behörden in Venezuela haben in Filialen der staatlichen Supermarktkette Bicentenario in Pitahaya südlich von Caracas am 09.03.2015 begonnen, Fingerabdruckscanner in Supermärkten zu installieren. Mit der Erfassung der biometrischen Daten der Einkaufenden sollen Hamsterkäufe verhindert und der Handel mit Lebensmitteln und Hygieneartikeln auf dem Schwarzmarkt bekämpft werden. Staatspräsident Nicolás Maduro erklärte, die Scanner seien ein „Segen“ im Kampf gegen den Schmuggel günstiger Lebensmittel aus Venezuela in die Nachbarstaaten: „Das biometrische System wird perfekt sein. Wir werden den Kampf gegen die Schmuggler und Schwarzmarkthändler gewinnen. Wir werden unser Volk, das arbeiten und in Ruhe leben will, gegen die Kapitalisten, Diebe, Individualisten und Kleinkriminellen verteidigen.“ Mit den Scannern soll festgestellt werden, ob einzelne Menschen ungewöhnlich häufig und viel einkaufen. Dahinter steht der Verdacht, dass die Kaufenden die Produkte außer Landes schmuggeln und dort zu höheren Preisen weiterverkaufen. Maduro kündigte an, in den folgenden Wochen würden 20.000 Scanner in Supermärkten installiert, zunächst vor allem im Grenzgebiet zu Kolumbien. Die Regierung teilte mit, auch die sieben größten privaten Supermarktketten hätten sich „freiwillig“ zur Einführung der Scanner bereitgefunden.

In den vorangegangenen Monaten hatten sich immer wieder lange Warteschlangen gebildet, wenn Lieferungen knapper Versorgungsgüter gemeldet wurden. Produkte wie Milch, Mehl und Zucker dürfen nur in begrenzten Mengen eingekauft werden. Mancherorts gibt es ein Rotationssystem, wonach die Menschen gemäß der Endzahl ihres Personalausweises einkaufen dürfen. Staatliche Preiskontrollen sorgen in Venezuela dafür, dass Lebensmittel und andere Produkte des täglichen Bedarfs teils nur ein Zehntel so viel kosten wie in den Nachbarstaaten. Maduro führt die grassierende Lebensmittelknappheit darauf zurück, dass in großem Stil günstige Produkte aus Venezuela herausgeschmuggelt werden, insbesondere nach Kolumbien. Seit kurzem schließt Venezuela jede Nacht die 2200 Kilometer lange Grenze zwischen beiden Ländern.

Oppositionspolitiker kritisierten den Scanner-Plan scharf und verglichen ihn mit kommunistischen Rationierungsmaßnahmen. Der oppositionelle Abgeordnete Alfonso Marquina erklärte: „Die Regierung kann Familien nicht einfach sagen, was sie essen sollen.“ Obwohl Venezuela die größten Ölreserven der Welt hat, steckt die Wirtschaft des Landes seit Langem in der Krise. Die Staatsverschuldung steigt, es gibt ständig Engpässe bei der Versorgung mit Grundnahrungsmitteln und anderen wichtigen Gütern. Die Inflation stand aufs Jahr gerechnet zuletzt bei 60% – von Sommer 2014 an veröffentlichte die Regierung keine neuen Zahlen mehr. US-Präsident Barack Obama erklärte, die sich verschlechternde Menschenrechtslage und die verbreitete Korruption in Venezuela seien eine Bedrohung für die nationale Sicherheit der Vereinigten Staaten (Venezuela erfasst Fingerabdrücke in Supermärkten, FAZ 10.03.2015, 6, Venezuela: Fingerabdruck-Scanner im Supermarkt, www.merkur-online.de 22.08.2014).

China

Onlinehandelsdaten für Bonitätsbewertung

Der Gründer und Eigner des chinesischen Online-Handels-Portals Alibaba Jack Ma entwickelt neue Geschäftsfelder, wofür er sich seiner E-Commerce-Daten bedient. Die chinesische Regierung in Peking hat nichts dagegen, im Gegenteil: Internetfirmen sollen dabei helfen, die Kreditwürdigkeit der Unternehmen und Menschen einzuschätzen.

Neuestes Produkt von Jack Mas Finanzkonzern Ant Financial Services ist ein Börsenindex, der 100 Premium-Aktien bewertet, die an chinesischen Börsen gehandelt werden, und der sich vornehmlich an Kleinanleger wendet. Im Juni 2015 nimmt außerdem die mit Alibaba verwandte Internetbank Mybank ihren Dienst in China auf. Sie will vor allem kleine und mittelständische Unternehmen mit Kapital versorgen. Yuan Leiming, Geschäftsführer von Ant Financial erläuterte: „Traditionelle Finanzdienstleister können nur wohlhabenden Kunden persönlich zugeschnittene Vermögensprodukte anbieten. Für einfache Leute haben sie nur standardisierte Produkte wie Sparkonten zur Verfügung.“ Der neue CSI Taojin 100 Index werde hingegen das Vertrauen der Anlegenden über Daten gewinnen, die normalen Finanzdienstleistern nicht zur Verfügung stehen, nämlich Informationen über Verkaufsvolumen, Preise, Angebot und Nachfrage von Produkten der bewerteten Firmen, die über die Online-Plattformen der Alibaba-Gruppe gesammelt werden. Dadurch soll dem Börsenbarometer ein entscheidender Wettbewerbsvorteil verschafft werden. Ant Financial Services wird zwar von Jack Ma und anderen Managern des IT-Unternehmens kontrolliert, doch wurde die Finanzsparte schon vor einigen Jahren ausgegliedert. Ma wollte damit offenbar verhindern, dass er bei seiner Expansion in die Finanzwelt von der chinesischen Aufsichtsbehörde gestoppt wird, da damals Yahoo ein Hauptinvestor war. Yahoo war von der Abspaltung nicht informiert worden und hatte deswegen später eine Abfindung kassiert.

Ant wie auch Alibabas IT-Rivale Tencent wollen eigene Online-Banken eröffnen. Mybank aus dem Alibaba-Umfeld, die im Juni 2015 ihr Geschäft aufnehmen möchte, und WeBank von Tencent gelten als echte Herausforderer traditioneller Großbanken. Perspektiven sehen die Wettbewerber vor allem im Kreditgeschäft. Private Firmen haben

es in China schwer, Kapital über eine Bankfinanzierung aufzunehmen, weil die Staatsbanken das höhere Risiko als bei staatlichen Unternehmen fürchten. Hier dienen Alibabas Online-Plattformen wie Taobao oder Tmall als Datensammelstellen für die Online-Bank. Anhand von Transaktionenvolumen, Käuferreaktionen oder Lieferzeiten soll Mybank umgehend für 10 Mio. Firmenkunden zugeschnittene Kreditangebote abgeben können. Yu Fenghui, der ein Buch über die „finanzielle Revolution" durch das Internet in China geschrieben hat, meint: „Die traditionellen Banken haben weder Zugriff auf diese Daten, noch können sie so schnell reagieren wie die Online-Banken". Yu vermutet, dass der Staat den Druck auf die herkömmlichen eher lethargen Finanzinstitute begrüßt: „Der Reformdruck wächst, deshalb versuchen sich große Staatsbanken wie die ICBC bereits darin, einen eigenen Online-Handel aufzuziehen."

Die Datengewinnung von Alibaba und Tencent interessiert auch die chinesische Zentralbank. Die PBOC forderte beide Unternehmen auf, sich am Aufbau eines Datensatzes über die Kreditwürdigkeit chinesischer BürgerInnen zu beteiligen. Alibaba hat in diesem Feld bereits erste Schritte unternommen. Das System „Zhima" ermittelt laut Technologie-Branchendienst 36kr die Summe, die eine KundIn bei Taobao oder Tmall von einem Kreditgeber risikofrei angeboten werden kann. Ziel ist es, InteressentInnen schon wenige Sekunden nach Anfrage eine Geldsumme zur Verfügung stellen zu können, die deren Kreditwürdigkeit entspricht (Grzanna, Heimvorteil, SZ 10.04.2015, 21).

Europa

Löschbeirat legt für Google-Suche Berichtsentwurf vor

Der Experten-Beirat, der sog. „Lösch-Beirat", des Internet-Konzerns Google hat nach sechsmonatiger Arbeit seinen Berichtsentwurf zum „Recht auf Vergessenwerden" geschrieben. Die ExpertInnen plädieren mehrheitlich dafür, Anträge auf Löschungen großzügiger als bisher zu handhaben. In seinem Google-Urteil vom 13.05.2014 gab der EU-Gerichtshof in Luxemburg den von Google-Suchanzeigen Betroffenen ein Recht auf Schutz ihrer Privatsphäre und einen Anspruch auf die Löschung von Links zu falschen oder kompromittierenden Daten. Die acht ExpertInnen, die Google dann als Beratende berufen hatte, begrüßen nun das Urteil mehrheitlich als wegweisend. Sie sprechen von einem Recht auf Geschütztsein im Internet und von einem Recht auf Versteckstsein vor der Suche im Netz. Dem unentgeltlich arbeitenden Gremium gehörten neben der früheren deutschen Bundesjustizministerin Sabine Leutheusser-Schnarrenberger (FDP) der UN-Sonderberichterstatter für Meinungsfreiheit Frank La Rue an, des weiteren Luciano Floridi, Professor für Informations-Ethik in Oxford, die frühere Le-Monde-Chefin Sylvie Kauffmann sowie der frühere spanische Datenschutzbeauftragte José-Luis Pinar, die polnische Juristin Lidia Kołucka-Żuk, Beraterin des früheren polnischen Ministerpräsidenten Donald Tusk; sowie Peggy Valcke, Professorin für Medienrecht an der Uni Leuven. Jimmy Wales, Mitbegründer von Wikipedia und Mitglied des Gremiums, sprach sich in den Beratungen immer wieder grundsätzlich gegen Löschansprüche aus. Er fordert das Europäische Parlament auf, den, wie er meint, sehr schlechten europäischen Rechtszustand zu verbessern und der Meinungsfreiheit mehr Gewicht zu geben. Bis dahin müsse man dem EU-Gerichtshof Folge leisten.

Uneinig sind sich die ExpertInnen über die Reichweite des Löschungsanspruchs: Sie plädieren mehrheitlich dafür, dass bei einem Anspruch auf Löschung von Links nur die Links auf EU-Domains gelöscht werden, wie es seit dem Luxemburger Gerichtsurteil schon Praxis bei Google ist. Die Löschung betrifft also nur die europäischen Varianten der Suche, also zum Beispiel Google.de oder Google.fr. Leutheusser-Schnarrenberger plädierte jedoch dafür, dass Google „global für alle Domains" löschen muss: „Wenn ich bei der Google-Suche in Europa über Google.com die Artikel wiederfinde, auf die sich der Löschungsanspruch bezieht, wird der Anspruch umgangen". Eine ähnliche Auffassung vertritt auch die sogenannte Artikel-29-Datenschutzgruppe, das Beratungsgremium der EU-Kommission für Fragen des Datenschutzes. Google ist strikt gegen einen so umfassenden Löschungsanspruch, weil er Auswirkungen auf den amerikanischen Markt hätte. Leutheusser-Schnarrenberger fordert den EU-Gesetzgeber auf, sich mit dieser Frage zu befassen. Die acht ExpertInnen, die Google nach dem Urteil des EU-Gerichtshofs bestellt hatte, sollten unter anderem eine Art „Lösch-Leitfaden" ausarbeiten, also Regeln und Empfehlungen zum Vorgehen bei komplizierten Löschanträgen.

Seit dem Urteil stellt der Suchmaschinenkonzern ein Online-Formular zur Verfügung, mit dem BürgerInnen beantragen können, Suchergebnisse aus dem Index zu nehmen. Der Experten-Beirat empfiehlt nun ein verbessertes Formular. Zudem sollen die Entscheidungen von Google über die Löschung differenzierter werden. Google soll sich auch nicht mehr, wie bisher üblich, für ein angebliches Interesse auf Information entscheiden. Es soll, so der Beirat, im Zweifel nicht gegen, sondern für die Löschung entschieden werden. Klare Kriterien, die jeweils für oder gegen Löschung sprechen, stellen die ExpertInnen nicht auf. Es komme auf die Gesamtbewertung an: Bei der Abwägung soll unter anderem eine Rolle spielen, ob die Antrag stellende Person die Information selbst preisgegeben hat. Der Zeitfaktor soll besonders bedeutsam sein: Je älter die Information, umso gewichtiger sei der Löschungsanspruch. Personen des öffentlichen Lebens sollen sich jedoch nicht so leicht reinwaschen können. Auch bei einer tatsächlich richtigen Berichterstattung soll es nach Meinung des Beirats ein Löschungsrecht geben – wenn die Fakten nicht mehr aktuell, nicht mehr relevant oder sehr privat sind. Eine Privatperson solle nämlich nicht ein Leben lang mit einem negativen Ereignis in Verbindung gebracht werden. Gemäß Leutheusser-Schnarrenberger hat der „Gedanke des Rechts auf eine zweite Chance" bei den Beratungen des Gremiums eine wichtige Rolle gespielt. Der eigentliche Text wird nicht gelöscht, er bleibt auffindbar; gelöscht werden nur die Links, die Hinweise auf diesen Text.

Bisher informiert Google bei jeder Löschung den Betreiber der betroffenen Seite, die Redaktion oder den Webmaster. Diesen Automatismus lehnt der

Experten-Beirat ab. Es müsse darauf geachtet werden, dass mit der Information über die Löschung nicht noch einmal das Datenschutzrecht missachtet werde – und der Seitenbetreiber also nicht noch einmal mit der Nase auf die inkriminierte Information gestoßen werde. Bei Google waren bis Januar 2015 seit dem Urteil des EU-Gerichtshofs ca. 205.000 Anträge auf Löschung eingegangen, 40% davon wurde stattgegeben. Aus Deutschland kamen ca. 35.000 Löschanträge, die Hälfte davon war erfolgreich. Das sind – bei 500 Millionen EU-BürgerInnen – weniger Löschanträge als erwartet. Leutheusser-Schnarrenberger plädiert dafür, dass Google für strittige Fälle eine unabhängige Schlichtung einführt, um der BürgerIn eine Klage zu ersparen.

Das Google-Gremium hatte von August bis November 2014 in sieben europäischen Städten Experten angehört. Diese Runden wurden zum Teil von Eric Schmidt, dem früheren Google-Chef und jetzigen Verwaltungsratsvorsitzenden des Konzerns moderiert; in Deutschland fand die Anhörung in Berlin statt. Auf dieser Basis und nach weiteren internen Beratungen in London wurde der Berichtsentwurf verfasst. Der Bericht soll das künftige Verhalten von Google bei Löschanträgen lenken und leiten (Prantl, Im Zweifel für die Löschung, http://jetzt.sueddeutsche.de/texte/anzeigen/591429/Im-Zweifel-fuer-die-Loeschung, 05.02.2015).

Technik-Nachrichten


Foto: Freddycat1 – Flickr.com

Sprechende „Barbie“ als Spitzel im Kinderzimmer

Eine neue, sprechende Barbie kann sich dank Sprachsoftware mit Kindern unterhalten – und speichert die Antworten beim Hersteller. Damit wird ein Kindertraum wahr: Schon bald kann Barbie beim Spielen ganz entspannt plaudern, wie eine echte Freundin. Banale Sprachausgaben auf Knopfdruck gehören der Vergangenheit an. Die im Februr 2015 offiziell vorgestellte sprechende Barbie ist schlauer: Ähnlich wie Apples iPhone-Assistentin „Siri“ ist sie per WLAN mit den Servern von Hersteller Mattel verbunden und kann ein richtiges Gespräch führen.

Die Barbie merkt sich jedes Wort, das um sie herum gesprochen wird. Das Kind kann mitteilen, wen es gerade mag, was es später für einen Job haben möchte... Tatsächlich hat Mattel angekündigt, dass Barbie auch die Berufsberatung übernehmen könne. Auf einem Server sind alle Gespräche gespeichert, die das Kind über sein Leben, seine Zukunft und seine Interessen mit Barbie führt. Die interessantesten Sachen landen in der Marketing-Abteilung von Mattel – oder sonst wo? Verkaufsstart der vernetzten Puppe soll noch im Jahr 2015 sein. Nicht bekannt ist, ob Mattel eine Schnittstelle für Eltern plant, mit der Ansagen an Barbie abgegeben werden können wie „Räum dein Zimmer auf!“ oder „Ab ins Bett“ oder „Wer war es?“-Verhöre von Geschwistern. Brigitte-Autor Hönicke hat die Vision, dass im Abo-Paket dann vielleicht sogar Antworten geliefert werden auf unbequeme Fragen wie „Warum kümmern sich meine Eltern so wenig um mich und übergeben den Job einer Puppe?“ (Hönicke, Spitzel im Kinderzimmer: Diese Barbie kann Kinder ausfragen und verpetzen, http://mom.brigitte.de/haben-wollen/sprechende-barbie-1233657/).

„BOSS Phone“ ermöglicht anonymes Browsen

Das von Designer David Briggs entwickelte Hightech-Smartphone „BOSS Phone“ ermöglicht dank Anbindung an das Tor-Netzwerk einen anonymen Datenverkehr. Mithilfe einer Kampagne auf der Crowdfunding-Plattform Indiegogo http://bit.ly/1tZ4cSX sucht das Projekt finanzielle Unterstützung. Das Handy soll ab Oktober 2015 für einen Preis von 355 Dollar (rund 300 Euro) verkauft werden.

Die User können Fotos und Videos hochladen, Anwendungen nutzen sowie E-Mails versenden, ohne dass eine dritte Partei dies zurückverfolgen kann. Mithilfe der App „Orbot“ http://bit.ly/1a15JMf funktioniert leicht die Einwahl in das Tor-Netzwerk. Briggs erklärt: „Dieses spezielle Netzwerk wird von ganz gewöhnlichen Menschen, dem Militär, Journalisten, Polizeibeamten, Aktivisten und jedem genutzt, der auf sicheres Kommunizieren und Browsen Wert legt.“ Neben der erhöhten Datensicherheit verfügt das BOSS Phone über ein sieben-Zoll-Display mit einer Auflösung von 1.920 mal 1.280 Pixel. Der interne Speicher beträgt 16 Gigabyte und kann dank einer MicroSD-Karte erweitert werden. Zusätzlich ist das BOSS Phone mit einem leistungsstarken Cortex-A7-Prozessor von Mediathek ausgestattet. Dem Entwickler zufolge beläuft sich die Akkulaufzeit auf mehr als 20 Stunden (Schmolmüller, „BOSS Phone“ ermöglicht anonymes Browsen, www.pressetext.com 12.01.2015).

Soziale Medien

IBM und Facebook kooperieren bei Werbung

Facebook und IBM haben am 06.05.2015 angekündigt, in Sachen personalisierter Werbung zusammenzuarbeiten. Werbetreibende sollen künftig zugleich aus zwei Quellen schöpfen können: aus dem „Audience Insights“-Tool von Facebook und aus „Interactive Marketing“ von IBM. Facebooks Vizepräsident Blake Chandler erklärte: „Wir beide wollen Menschen und Marken zusammenbringen. In diesem Ziel sind wir einander verbunden. Außerdem haben wir einige große gemeinsame Kunden.“ Bei der Kooperation geht es insbesondere darum, das Datenanalyse-Geschäft von IBM mit den aus Marketingsicht wertvollen Userinformationen von Facebook zu verschmelzen.

IBM bietet Händlern und Marken Marketinginstrumente an; dabei werden etwa Webseiten-Besuche oder Anrufe bei Kunden-Hotlines registriert. Das soziale Netzwerk kennt die Vorlieben seiner Nutzenden, so IBM-Manager Deepak Advani: „Unser Kunden haben uns gedrängt, Facebook einzubeziehen, weil es so wichtig ist. Auf Facebook verbringen Konsumenten einen großen Teil ihrer Zeit.“ Früher konnten Werbetreibende Menschen nur aufgrund grober demographischer Merkmale wie Alter, Geschlecht, Einkommen oder Wohnort ansprechen. Moderne Methoden ermöglichen es, auch in sehr kleinen Milieus potentielle KundInnen auszumachen. IBM erhofft sich durch die Kooperation Zuwachs bei seiner E-Commerce-Sparte. Facebook verspricht sich laut Chandler, „effektivere“ Werbung in dem sozialen Netzwerk zu schalten, um damit attraktiver für Anzeigenkunden zu werden und behauptete: „Persönliche Daten werden nicht hin und her gereicht“. Mit konkreten Namen und E-Mail-Adressen würde nicht gearbeitet. Dass dabei nach europäischem Datenschutzrecht personenbezogene Daten verarbeitet werden, ist jedoch diesseits des Ozeans unstreitig (IBM und Facebook wollen gemeinsam Werbung personalisieren, http://www.sueddeutsche.de 06.05.2015; IBM und Facebook schmieden Werbepakt, http://www.computerwelt.at 06.05.2015).

Für Rachepornos droht Haft

Mitte Februar 2015 wurde in Großbritannien eine Gesetzesänderung angekündigt, die für Rachepornos maximal zwei Jahre Haft vorsieht. Dies gelte für Fotos oder Filme, die ohne Zustimmung des Ex-Partners im Internet oder per SMS verbreitet würden und Menschen bei “sexuellen Aktivitäten oder in sexuellen Posen oder mit entblößten Genitalien” zeigen. Die Verschärfung soll über eine Ergänzung zum Criminal Justice and Courts Bill erfolgen. Justizminister Chris Grayling erklärte: “Wir wollen denjenigen, die Opfer dieser Art ekelhaften Verhaltens geworden sind, wissen lassen, dass wir auf ihrer Seite stehen.” Britische Nudisten haben sich dagegen gewandt, dass damit auch Fotos von Freunden und Familie an Nacktbadestränden unter Strafe gestellt werden.

Das deutsche Bundesjustizministerium teilte auf Anfrage mit, dass die Verbreitung von intimen Bildern ohne die Zustimmung der gezeigten Person in Deutschland bereits unter Strafe gestellt sei. Revenge-Porn-Plattformen veröffentlichen private pornografische Bilder oder Nacktaufnahmen mit dem vollen Namen und der Adresse der Opfer. Anbei stehen oft Links zu ihren Profilen auf sozialen Netzwerken. Oft werden aus Rache auch in sozialen Netzwerken pornografische Aufnahmen von früheren Partnern ohne Zustimmung veröffentlicht. Die Regierung verweist auf § 22 des Kunsturhebergesetzes (KUG), der die Einwilligung des Abgebildeten für die Verbreitung und Veröffentlichung von Bildern voraussetzt: “Dabei ist auch zu beachten, dass eine wirksam erteilte Einwilligung räumlich, zeitlich oder inhaltlich beschränkt sein kann und so nicht jegliche Verbreitung abdeckt. Darüber hinaus ist eine Anfechtung und auch ein Widerruf einer Einwilligung zulässig.” Bei Verstößen drohe nach § 33 des Gesetzes eine Freiheitsstrafe von bis zu einem Jahr oder eine Geldstrafe. Zudem habe das Bundeskabinett kürzlich einen Gesetzentwurf zur Verschärfung des Strafgesetzbuches (StGB) beschlossen. Dieser sieht eine Geldstrafe oder Freiheitsstrafe von bis zu zwei Jahren für denjenigen vor, “der unbefugt von einer anderen Person eine Bildaufnahme macht, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, oder der unbefugt eine Bildaufnahme von einer unbekleideten anderen Person herstellt oder überträgt”. Darüber hinaus ist eine Freiheitsstrafe von bis zu drei Jahren oder eine Geldstrafe vorgesehen, wenn solche Bildaufnahmen verbreitet oder veröffentlicht werden. Diese Tatbestände könnten, so das Ministerium, durch “Rachepornos” erfüllt sein.

Betroffene können sich zudem zivilrechtlich gegen solche Veröffentlichungen wehren und Ansprüche auf Beseitigung und Unterlassung geltend machen. Schadenersatzansprüche lassen sich aus § 823 Abs. 1 des Bürgerlichen Gesetzbuches ableiten. “Bei einer schwerwiegenden Verletzung des allgemeinen Persönlichkeitsrechts kann eine Geldentschädigung für immaterielle Schäden gefordert werden, wenn die Beeinträchtigung nicht in anderer Weise befriedigend ausgeglichen werden kann.” Auch gegen die Plattform, die die Bilder oder Videos veröffentlicht habe, könne vorgegangen werden. Sie ist laut § 10 des Telemediengesetzes verpflichtet, das Material zu entfernen, wenn sie über eine Rechtsverletzung Kenntnis erlangt hat. Über diese Gesetze hinaus will die Regierung keine neuen Regelungen wegen “Rachepornos” erlassen (Haft für “Rachepornos”, SZ 13.02.2015, 10; Sawall/Greis, Bei Rachepornos drohen in Deutschland drei Jahre Haft, www.golem.de 16.02.2015).

Rechtsprechung

EGMR

Medien kann versteckte Kamera erlaubt sein

Der Europäische Gerichtshof für Menschenrechte (EGMR) in Straßburg entschied mit Urteil vom 24.02.2015, dass JournalistInnen für ihre Recherche versteckte Kameras verwenden dürfen, und gab damit mit Hinweis auf die Freiheit der Meinungsäußerung nach Art. 10 der Europäischen Menschenrechtskonvention (EMRK) zwei schweizer Journalisten Recht, die zuvor in der Schweiz zu Geldstrafen verurteilt worden waren. Sie hatten für das schweizerische Fernsehformat „Kassensturz", ein wöchentliches Sendeformat zum Thema Verbraucherschutz, mit zwei weiteren Journalisten und in Absprache mit den Redaktionschefs einen Versicherungsmakler von Lebensversicherungen interviewt und mit versteckter Kamera gefilmt, um die zweifelhaften Methoden und irreführenden Beratungsweisen der Verkäufer aufzudecken und zu dokumentieren. Die versteckten Kameras wurde zuvor im Interviewraum installiert. Im Nebenzimmer verfolgten u. a. die beiden Redaktionschefs die Szenerie, da das Interview dorthin übertragen wurde. Nach Beendigung des Interviews betrat einer der beiden Redaktionschefs den Interviewraum, um den Versicherungsmakler über die heimliche Aufnahme zu informieren. Bei Ausstrahlung der Sendung im März 2003 wurde das Gesicht des Maklers unkenntlich gemacht und seine Stimme verändert.

Im November 2007 wurden die Journalisten wegen der Aufnahmen mit versteckter Kamera durch das Zürcher Obergericht zu Geldstrafen verurteilt. Auf die Klage der Journalisten hin hob der EGMR das Urteil mit der Begründung auf, dass das öffentliche Interesse an Informationen über angebliche dubiose Praktiken beim Verkauf von Versicherungen wichtiger sei als der Schutz der Privatsphäre des Maklers. Durch die Verurteilung der vier Journalisten sei eine Verletzung der Freiheit der Meinungsäußerung nach Art 10 EMRK gegeben. Danach hat jeder das Recht auf freie Meinungsäußerung. Das Recht schließt die Meinungsfreiheit und die Freiheit ein, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben. Durch ein Urteil wie das des Zürcher Obergerichts könnten Medien von kritischen Beiträgen abgehalten werden, auch wenn sie nicht daran gehindert würden, den Beitrag auszustrahlen. Entscheidend für den EGMR war, dass in der Sendung das Gesicht des Versicherungsmaklers unkenntlich gemacht und seine Stimme verfremdet wurden. Zudem sei die Kamera außerhalb der Büroräume des Maklers eingesetzt worden.

Das Berichterstattungsinteresse kollidiert regelmäßig mit geschützten Rechten der von diesen ins Visier genommenen Personen, was oftmals strafrechtlich oder zivilrechtlich geahndet werden kann. Erfolgt diese gemäß den allgemeinen Gesetzen, so besteht ein Konflikt zwischen diesen und der verfassungsrechtlich besonders gewährleisteten und geschützten Pressefreiheit. Unter welchen Voraussetzungen ein öffentliches Informationsinteresse gegenüber den Rechten des Betroffenen überwiegt, bedarf grundsätzlich der Abwägung des Einzelfalles, was für recherchierende Journalisten zu Unsicherheiten führt. Insofern gibt das ergangene Urteil wichtige Hinweise (Solmecke, Versteckte Kamera – EGMR erlaubt Medien den Einsatz, www.wbs-law.de 25.02.2015).

BGH

Hinweis auf mögliche Schufa-Meldung nur bei korrekter Aufklärung zulässig

Der für das Wettbewerbsrecht zuständige I. Zivilsenat des Bundesgerichtshofs (BGH) hat mit Urteil vom 19.03.2015 festgehalten, unter welchen Voraussetzungen ein Hinweis von Unternehmen in Mahnschreiben an ihre Kunden auf eine bevorstehende Mitteilung von Schuldnerdaten an die Schufa unzulässig ist (I ZR 157/13 – Schufa-Hinweis).

Die Verbraucherzentrale (VZ) Hamburg e.V. hatte gegen ein Mobilfunkunternehmen geklagt, das sich zum Einzug von nicht fristgerecht bezahlten Forderungen eines Inkassoinstituts bedient. Das Inkassoinstitut übersandte an Kunden der Mobilfunkunternehmen Mahnschreiben, in denen es unter anderem hieß: „Als Partner der Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) ist die V. GmbH verpflichtet, die unbestrittene Forderung der Schufa mitzuteilen, sofern nicht eine noch durchzuführende Interessenabwägung in Ihrem Fall etwas anderes ergibt. Ein Schufa-Eintrag kann Sie bei Ihren finanziellen Angelegenheiten, z. B. der Aufnahme eines Kredits, erheblich behindern. Auch Dienstleistungen anderer Unternehmen können Sie dann unter Umständen nicht mehr oder nur noch eingeschränkt in Anspruch nehmen."

Die VZ sah in dem Hinweis auf die Pflicht zur Meldung der Forderung an die Schufa eine unangemessene Beeinträchtigung der Entscheidungsfreiheit der Verbraucher (§ 4 Nr. 1 UWG). Sie forderte vom Mobilfunkunternehmen die Unterlassung des Hinweises. Das Landgericht hatte die Klage der VZ abgewiesen. Das Oberlandesgericht (OLG) hatte dann das Mobilunternehmen auf die Berufung der VZ hin antragsgemäß verurteilt. Es hat einen Verstoß gegen § 4 Nr. 1 UWG bejaht. Der BGH hat die hiergegen vom Mobilfunkunternehmen eingelegte Revision zurückgewiesen. Das OLG habe zutreffend angenommen, dass das beanstandete Mahnschreiben beim Adressaten den Eindruck erweckt, er müsse mit einer Übermittlung seiner Daten an die Schufa rechnen, wenn er die geltend gemachte Forderung nicht

innerhalb der gesetzten Frist befriedige. Wegen der einschneidenden Folgen eines Schufa-Eintrags bestehe die Gefahr, dass Verbraucher dem Zahlungsverlangen des Mobilfunkunternehmens auch dann nachkommen, wenn sie die Rechnung wegen tatsächlicher oder vermeintlicher Einwendungen eigentlich nicht bezahlen wollten. Damit besteht die konkrete Gefahr einer nicht informationsgeleiteten Entscheidung der Verbraucher, die die Zahlung nur aus Furcht vor der Schufa-Eintragung vornehmen.

Die beanstandete Ankündigung der Übermittlung der Daten an die Schufa sei auch nicht durch die gesetzliche Hinweispflicht nach § 28a Abs. 1 Nr. 4 Buchst. c Bundesdatenschutzgesetz (BDSG) gedeckt. Zu den Voraussetzungen der Übermittlung personenbezogener Daten nach dieser Vorschrift gehört, dass der Betroffene die Forderung nicht bestritten hat. Ein Hinweis auf die bevorstehende Datenübermittlung stehe nur dann im Einklang mit der Bestimmung, wenn nicht verschleiert wird, dass ein Bestreiten der Forderung durch den Schuldner selbst ausreicht, um eine Übermittlung der Schuldnerdaten an die Schufa zu verhindern. Diesen Anforderungen entsprach der beanstandete Hinweis des beklagten Mobilfunkunternehmens nicht (PM BGH Nr. 40/2015 19.03.2015, Bundesgerichtshof zum Hinweis auf die bevorstehende Mitteilung von Schuldnerdaten an die SCHUFA in Mahnschreiben).

BAG

Detektiv-Observation mit heimlichen Videoaufnahmen unzulässig

Das Bundesarbeitsgericht (BAG) in Erfurt hat mit Urteil vom 19.02.2015 entschieden, dass ein Arbeitgeber, der wegen des Verdachts einer vorgetäuschten Arbeitsunfähigkeit einem Detektiv die Überwachung einer Arbeitnehmerin überträgt, rechtswidrig handelt, wenn sein Verdacht nicht auf konkreten Tatsachen beruht (8 AZR 1007/13). Für dabei heimlich hergestellte Abbildungen gilt dasselbe. Eine solche rechtswidrige Verletzung des allgemeinen Persönlichkeitsrechts kann einen Geldentschädigungsanspruch („Schmerzensgeld") begründen.

Die Klägerin war bei dem beklagten Arbeitgeber seit Mai 2011 als Sekretärin der Geschäftsleitung in einem kleinen Betrieb mit 18 Beschäftigten tätig. Ab dem 27.12.2011 war sie arbeitsunfähig erkrankt, zunächst mit Bronchialerkrankungen. Für die Zeit bis 28.02.2012 legte sie nacheinander sechs Arbeitsunfähigkeitsbescheinigungen vor, zuerst vier eines Facharztes für Allgemeinmedizin, dann ab 31.01.2012 zwei einer Fachärztin für Orthopädie. Der Geschäftsführer des Arbeitgebers bezweifelte den zuletzt telefonisch mitgeteilten Bandscheibenvorfall und beauftragte einen Detektiv mit der Observation der Klägerin. Diese erfolgte von Mitte bis Ende Februar 2012 an vier Tagen. Beobachtet wurden u. a. das Haus der Klägerin, sie und ihr Mann mit Hund vor dem Haus und der Besuch der Klägerin in einem Waschsalon. Dabei wurden auch Videoaufnahmen erstellt. Der dem Arbeitgeber übergebene Observationsbericht enthält elf Bilder, neun davon aus Videosequenzen, u. a. zu einer Situation in einem Waschsalon, wie die Frau „im Hocken" eine Waschmaschine befüllte. Mit dem Material rechtfertigte der Arbeitgeber die fristlose Kündigung der Frau. Die Klägerin, die 3.500 Euro im Monat verdiente, hielt die Beauftragung der Observation einschließlich der Videoaufnahmen für rechtswidrig und forderte ein Schmerzensgeld in Höhe von 10.500 Euro. Die Klägerin habe erhebliche psychische Beeinträchtigungen erlitten, die ärztlicher Behandlung bedürften. Die Sekretärin hatte sich gegen die Verdächtigung u. a. mit der Aussage gewehrt, sie habe im Waschsalon in die Hocke gehen können, weil es ein Bandscheibenunfall in der Halswirbelsäule und nicht weiter unten gewesen sei.

Das Landesarbeitsgericht (LAG) Hamm hatte der Klage mit Urteil vom 11.07.2013 in Höhe von 1.000,00 Euro stattgegeben (11 Sa 312/13). Auch gegen ihren Rausschmiss hatte sie sich juristisch gewehrt und schon vor dem Arbeitsgericht und dem LAG Recht bekommen. Die Revisionen beider Parteien blieben vor dem BAG ohne Erfolg. Dieses bestätigte die Rechtswidrigkeit der Observation einschließlich der heimlichen Aufnahmen. Der Arbeitgeber habe keinen berechtigten Anlass zur Überwachung gehabt. Der Beweiswert der Arbeitsunfähigkeitsbescheinigungen war weder dadurch erschüttert, dass sie von unterschiedlichen Ärzten stammten, noch durch eine Änderung im Krankheitsbild oder weil ein Bandscheibenvorfall zunächst hausärztlich behandelt worden war. Die vom LAG angenommene Höhe des Schmerzensgeldes wurde revisionsrechtlich nicht korrigiert. Das BAG traf keine Entscheidung darüber, wie Videoaufnahmen zu beurteilen sind, wenn ein berechtigter Anlass zur Überwachung gegeben ist (Esslinger, Von Chefs und Detektiven, SZ 20.02.2015, 6; PE BAG 19.02.2015, Observation durch einen Detektiv mit heimlichen Videoaufnahmen).

LVerfG LSA

Technisch noch nicht mögliche Eingriffe dürfen nicht geregelt werden

Das Landesverfassungsgericht Sachsen-Anhalt (LVerfG LSA) hat mit Urteil vom 11.11.2014 einem Normenkontrollantrag der Abgeordneten der Fraktionen Die Linke und Bündnis 90/Die Grünen des Landtages von Sachsen teilweise stattgegeben, mit dem die Änderung des Polizeirechts des Landes, konkret das Vierte Gesetz zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt (SOG LSA) vom 26.03.2013, angegriffen wird (LVG 9/13).

Das Gericht erklärte die Regelung des § 17c SOG LSA für nichtig, die es der Polizei zur Gefahrenabwehr erlaubte, ohne Wissen der betroffenen Personen Telekommunikationsinhalte und -umstände durch den Einsatz technischer Mittel zu erheben. Es erkannte an, dass der Gesetzgeber mit der Vorschrift einen legitimen Zweck verfolgt. Da jedoch die technischen Voraussetzungen derzeit noch nicht geschaffen sind, konnte der Gesetzgeber die hierfür erforderliche verantwortliche Abwägungsentscheidung noch nicht treffen: „Der Einsatz technischer Instrumente zu Zwecken der Telekommunikationsüberwachung verlangt eine gesetzliche Grundlage, die der Gesetzgeber in Kenntnis der Eigen-

schaften der technischen Instrumente durch eine Abwägungsentscheidung getroffen hat und damit verantworten kann. Existieren die technischen Instrumente zum Zeitpunkt der Gesetzgebung noch nicht, muss der Gesetzgeber durch verfahrensrechtliche Vorgaben sicherstellen, dass eine verantwortliche Prüfung der Eignung der technischen Instrumente erfolgt.“

Bestätigt hat das LVerfG den § 33 SOG LSA, der der Polizei die Unterbrechung und Verhinderung von Kommunikationsverbindungen gestattet: „Die Unterbrechung oder Störung von Kommunikationsverbindungen zum Zweck der Abwehr von Gefahren für Leib, Leben oder Freiheit von Personen ist verfassungsrechtlich auch gegenüber Personen zulässig, von denen keine Gefahr ausgeht, wenn die Gefahrenabwehr anderenfalls nicht möglich ist. Eine solche Maßnahme stellt auch dann keinen Eingriff in das Grundrecht der Versammlungsfreiheit dar, wenn faktisch die Organisatoren oder Teilnehmer von Versammlungen durch die Maßnahme betroffen sind.“

Hinsichtlich der Videoaufzeichnung bei Personen- und Fahrzeugkontrollen, weiterer Regelungen zur Erhebung von Telekommunikationsinhalten und -umständen sowie der Untersuchung von Personen mit potentiell gefährlichen Krankheitserregern hat das Gericht dem Gesetzgeber aufgegeben, bis zum 31.12.2015 verfassungskonforme Neuregelungen zu schaffen. Bis dahin sind die Vorschriften nach Maßgabe des Urteils anwendbar (PE Nr. 011/14 LVerfG LSA vom 11.11.2014, Regelungen zur Änderung des Gesetzes über die öffentliche Sicherheit und Ordnung des Landes Sachsen-Anhalt vom 26. März 2013 teilweise verfassungswidrig).

BayVGH

Funktionsträgerdaten vor Internetveröffentlichung geschützt

Gemäß einem Urteil des Bayerischen Verwaltungsgerichtshofs (BayVGH) vom 26.03.2015 dürfen Namen und Kontaktdaten von Angehörigen des öffentlichen Dienstes, also von öffentlichen FunktionsträgerInnen, nicht nach Belieben im Internet veröffentlicht werden (Az.: 5 B 14.2164). Damit wurde die Klage der Wählergemeinschaft Freie Liste Zukunft (Flitz) aus Neumarkt in der Oberpfalz endgültig abgewiesen, die auf ihrer Internetseite Namen und diverse Kontaktdaten einer Mitarbeiterin des Landesamts für Umwelt genannt hatte. Flitz wollte damit Schwierigkeiten bei der Nachforschung nach Umweltdaten dokumentieren. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hatte daraufhin die Löschung der personenbezogenen Daten gefordert; hiergegen hatte Flitz geklagt. Die Wählergemeinschaft rechtfertigte die Namensveröffentlichung damit, es solle so den LeserInnen der Internetseite klar gemacht werden, auf welche Schwierigkeiten Flitz bei der Nachforschung nach Umweltdaten gestoßen sei. Man sei falsch informiert worden und in der Verweisung von einem Sachbearbeitenden an den anderen liege eine systematische Fehlleistung der Behörde insgesamt vor. Es sei nötig, den Nachnamen des jeweils betroffenen Sachbearbeitenden zu veröffentlichen, da diesem in seiner Funktion ein Vorwurf zu machen sei.

Die 9. Kammer des BayVGH stellte fest, dass die Behördenangestellte nicht in ihrer Privat-, sondern in ihrer Sozialsphäre betroffen ist, wenn diese Daten einer weltweiten Öffentlichkeit zugänglich gemacht werden. Äußerungen von Mitarbeitenden seien grundsätzlich den jeweiligen Behörden zuzurechnen, in deren Auftrag sie handeln. Wer als SachbearbeiterIn einer Angelegenheit tätig geworden ist, sei nur von untergeordneter Bedeutung. Dies gelte erst recht im entschiedenen Fall, da die Mitarbeiterin im Bürgerreferat des Umweltministeriums lediglich Anfragen an die einzelnen Fachreferate weitergegeben habe (Müller-Jentsch, Gericht weist Flitz-Klage ab, SZ 27.03.2015, 46).

OVG Hamburg

Regelung zu Gefahrengebieten verfassungswidrig

Das Hamburgische Oberverwaltungsgericht (OVG) hat mit Urteil vom 13.05.2015 die gesetzliche Grundlage für die Ausweisung von Gefahrengebieten in Hamburg für verfassungswidrig erklärt (4 Bf 226/12). Hintergrund des Verfahrens ist die Ausweisung eines Gefahrengebiets im Schanzenviertel in Hamburg anlässlich der sog. Walpurgisnacht am 30.04/01.05.2011. Die Polizei überprüfte am 30.04. die Identität der Klägerin und kontrollierte ihren Rucksack. Anschließend erhielt sie ein Aufenthaltsverbot und wurde bis in die frühen Morgenstunden des Folgetages in Gewahrsam genommen. Im nachfolgenden Klageverfahren stellte das Verwaltungsgericht (VG) fest, dass das Aufenthaltsverbot und die Ingewahrsamnahme der Klägerin rechtswidrig gewesen seien. Die zuvor erfolgte Identitätsfeststellung und die Kontrolle des Rucksacks seien demgegenüber rechtens gewesen.

Das OVG entschied im Berufungsverfahren, dass auch die Identitätsfeststellung und die Kontrolle des Rucksacks rechtswidrig waren. Die gesetzliche Grundlage in § 4 Abs. 2 des Gesetzes über die Datenverarbeitung der Polizei (HmbPolDVG) sei verfassungswidrig. Sie verstoße gegen das rechtsstaatliche Bestimmtheitsgebot und gegen den Grundsatz der Verhältnismäßigkeit. Sie gebe zum einen nicht klar genug die Voraussetzungen für die Ausweisung eines Gefahrengebiets vor. Vielmehr bleibe es weitgehend der Polizei überlassen zu entscheiden, ob und für wie lange ein Gefahrengebiet ausgewiesen und dort Personen verdachtsunabhängig überprüft werden könnten. Das Gesetz erlaube Eingriffsmaßnahmen von erheblichem Gewicht zur Abwehr bloß abstrakter Gefahren und gegenüber Personen, ohne dass diese zuvor einen konkreten Anlass für eine gegen sie gerichtete polizeiliche Maßnahme gegeben haben müssen. Die hiermit verbundene Belastung sei nicht angemessen.

Im konkreten Fall seien die gegen die Klägerin gerichteten Maßnahmen aber auch aus anderen Gründen rechtswidrig gewesen. Bei der Kontrolle des Rucksacks habe es sich um eine Durchsuchung gehandelt, die von § 4 Abs. 2 HmbPolDVG nicht gedeckt sei. Die Vorschrift erlaube nur die Inaugenscheinnahme mitgeführter Sachen. Die Auswahl der Klägerin zu einer Kontrollmaßnahme sei zudem ermessensfehlerhaft gewesen, denn der Auswahl habe

ein unzulässiges, weil ungeeignetes Unterscheidungskriterium („linkes Spektrum“) zugrunde gelegen (Oberverwaltungsgericht hält Gefahrengebiete für verfassungswidrig, PM Hamburgisches Oberverwaltungsgericht 13.05.2015, http://justiz.hamburg.de/contentblob/4496240/data/4bf226-12.pdf).

OVG NRW

Kein informationsrechtlicher Anspruch auf richterliche Telefonliste

Das Oberverwaltungsgericht (OVG) Nordrhein-Westfalen in Münster hat mit Urteil vom 06.05.2015 entschieden, dass das Land Nordrhein-Westfalen nicht nach dem Informationsfreiheitsgesetz Nordrhein-Westfalen (IFG NRW) verpflichtet ist, auf Antrag Zugang zur vollständigen Telefonliste des Verwaltungsgerichts (VG) Aachen zu gewähren (8 A 1943/13). Das OVG wies damit die Klage eines Rechtsanwalts ab, soweit diese auf die Herausgabe der Durchwahlnummern aller Richterinnen und Richter gerichtet war. Soweit die Telefonnummern der nichtrichterlichen Gerichtsangehörigen betroffen waren, hat der Senat die ablehnende Entscheidung des (vormaligen) Präsidenten des Verwaltungsgerichts Aachen aufgehoben und das beklagte Land verpflichtet, den Antrag unter Beachtung der Rechtsauffassung des Gerichts neu zu bescheiden.

In der mündlichen Begründung führte der Senats-Vorsitzende des OVG aus, dass kein allgemeiner Anspruch auf Bekanntgabe der Durchwahlnummern aller RichterInnen bestehe. Der Anspruch sei nach § 6 Satz 1 Buchst. a IFG NRW ausgeschlossen. Zu den von dieser Vorschrift erfassten Schutzgütern der öffentlichen Sicherheit zähle auch die Funktionsfähigkeit der staatlichen Einrichtungen. Die RichterInnen des VG Aachen seien – vergleichbar der Übung in den meisten Anwaltskanzleien oder Arztpraxen – nicht direkt über ihre Durchwahlnummer, sondern über die jeweilige SekretärIn bzw. Service-Einheit erreichbar. Die Telefonnummern der Service-Einheiten ergäben sich aus der Internetseite des VG Aachen. Diese Entscheidung des Gerichtspräsidenten diene dem Ziel, die Anrufer gezielt zu führen, ihre Telefonanrufe nach sachlichen Anliegen zu sortieren sowie fachkompetent und arbeitsteilig zu beantworten. Damit solle eine effektive Aufgabenerledigung sichergestellt werden. Das Antragsziel, diese gerichtsintern vorgesehenen Arbeitsabläufe durch Anrufe direkt bei RichterInnen zu umgehen, könne zu einer nachhaltigen Störung der richterlichen Arbeit führen.

Hinsichtlich der Telefonnummern der nichtrichterlichen Gerichtsangehörigen seien öffentliche Belange nicht betroffen. Der Zugang zu diesen Telefonnummern scheitere aber am Schutz personenbezogener Daten, weil bzw. solange die betroffenen Gerichtsangehörigen nicht in die Weitergabe ihrer Telefondaten eingewilligt hätten. Das Gesetz verpflichte in diesem Fall dazu, die Betroffenen personenbezogen nach ihrer Einwilligung zu befragen. Dies sei bisher nicht geschehen. Der ablehnende Bescheid sei daher insoweit aufzuheben und der Beklagte zu verpflichten gewesen, den Kläger nach Durchführung der Drittbeteiligung neu zu bescheiden. Der Senat hat die Revision nicht zugelassen. Dagegen ist eine Nichtzulassungsbeschwerde möglich, über die das Bundesverwaltungsgericht entscheidet (Klage eines Rechtsanwalts auf Herausgabe der Telefondurchwahlnummern aller Richter ohne Erfolg, PE OVG Münster 06.05.2015).

OLG Köln

Abdruck von Kohl-Zitaten unzulässig

Der 15. Zivilsenat des Oberlandesgerichts (OLG) Köln entschied am 05.05.2015, dass die Verwendung und Veröffentlichung von Zitaten Dr. Helmut Kohls in dem Buch „Vermächtnis – die Kohl-Protokolle“ unzulässig ist und wies die Berufung der Beklagten gegen ein Urteil des Landgerichts (LG) Köln vom 13.11.2014 zurück (15 U 193/14). In den Buchläden war das Buch nur noch verfügbar mit einem gelben Sticker auf dem Cover: „Mit den offiziell vom Landgericht Köln erlaubten Passagen.“ Das LG hatte entschieden, dass die Beklagten – die Autoren Dr. Heribert Schwan und Tilman Jens sowie der Verlag Random House – den überwiegenden Teil der Zitate, die dem Autor Herrn Dr. Schwan im Rahmen seiner Arbeit an den Memoiren des Klägers zwischen 2000 und 2001 zur Verfügung gestellt wurden, nicht weiter verwenden und veröffentlichen dürfen. Das OLG bestätigte nicht nur das Urteil des LGs, sondern ging mit der Berufung der Kläger mit dem Verbot weiterer Zitate über das Urteil der Vorinstanz hinaus, die noch für zulässig erachtet wurden.

Nach Ansicht des OLG war den Beklagten die Veröffentlichung sämtlicher 115 Zitate, die Gegenstand des Berufungsverfahrens waren, verboten. Darunter befinden sich Äußerungen über die Politiker Christian Wulff, Richard von Weizäcker, Klaus Töpfer und Palästinenserführer Jassir Arafat. Den Beklagten zu 2) – Herr Dr. Schwan – habe eine vertragliche Pflicht zur Geheimhaltung getroffen, die im Rahmen der Vereinbarung der Zusammenarbeit zur Erstellung der Biographien Herrn Dr. Kohls konkludent verabredet worden sei und Herrn Dr. Schwan hindern sollte, die auf den Tonbändern fixierten Äußerungen ohne Einverständnis des Klägers zu veröffentlichen. Die Pflicht ergebe sich aus dem besonderen Gefüge der Verträge zwischen dem Drömer Verlag und Kohl bzw. dem Verlag und Schwan, insbesondere den darin den Parteien zugewiesenen Funktionen und Befugnissen. So sollte Herr Dr. Kohl die Entscheidungshoheit über die Verwendung seiner Äußerungen als solche sowie den konkreten Inhalt und den Zeitpunkt der Veröffentlichung zustehen. Herr Dr. Schwan hingegen sei als Ghostwriter eine lediglich dienende Funktion zugewiesen worden. Zudem folge die Geheimhaltungsverpflichtung aus der Zweckbindung der Tonbandaufzeichnungen als lediglich allgemeiner Stoffsammlung für die geplanten Memoiren. Mit der Geheimhaltungsabrede habe der Beklagte zu 2) auf sein diesbezügliches Recht auf freie Meinungsäußerung verzichtet. Es sei eine „stillschweigenden Geheimnisvereinbarung“ anzunehmen. Mehr als 600 Stunden hatten beide sich in Kohls Haus unterhalten; Schwan schrieb auf dieser Grundlage als Ghostwriter drei Bände der Memoiren. Vor dem letzten – in ihm sollte es um den

Sturz und die Spendenaffäre gehen – beendete Kohl die Zusammenarbeit und forderte die Bänder zurück. Schwan ging zum Random Verlag und veröffentlichte große Teile der Gespräche.

Die Beklagten zu 1) und 3) – Tilman Jens und der Verlag Random House – hätten die maßgeblichen Äußerungen ebenfalls nicht veröffentlichen dürfen. Dieses Unterlassungsgebot folge nicht aus einer vertraglichen Bindung, sondern aus der Verletzung des allgemeinen Persönlichkeitsrechts des Klägers in Form der Vertraulichkeitssphäre und des Rechts am gesprochenen Wort. Zum Schutz der Pressefreiheit sei zwar nicht jede Veröffentlichung rechtswidrig erlangter Informationen ausgeschlossen. Ein absolutes Verwertungsverbot bestehe aber dann, wenn Tonbandaufzeichnungen in wörtlicher Rede ungenehmigt weitergegeben werden sowie dann, wenn sich die Presse über die schützenswerten Belange des Betroffenen hinwegsetze.

Den Beklagten zu 1) und 3) seien sowohl die konkreten Umstände bekannt gewesen, unter denen der Beklagte zu 2) die vertraulich erfolgten Äußerungen des Klägers aufgenommen habe, als auch das spätere Zerwürfnis, welches eine weitere Zusammenarbeit beendet habe. Zudem seien sie an der Erstellung des streitgegenständlichen Buches verantwortlich beteiligt gewesen. Die Beklagten hätten selbst stets betont, bei der Entwicklung des Buchprojekts durchgängig als Team gewirkt zu haben. So hätten sie bei der Auswahl der Inhalte zusammengearbeitet, diese gemeinsam redigiert und die Texte ausgeformt. Diese Art der Informationsgewinnung und -verwertung stehe einer weiteren Verwendung und Veröffentlichung entgegen. Richter Andreas Zingsheim erläuterte sein Urteil: „Schwan war Zuarbeiter, die letzte Entscheidung, was veröffentlicht werden sollte, lag bei Helmut Kohl.“ Schwan, sein Co-Autor Jens und Random House hätten sich „in rücksichtsloser Weise über die schützenswerten Belange des Betroffenen hinweggesetzt.“

Ein Rechtsmittel gegen die im einstweiligen Verfügungsverfahren ergangene Entscheidung ist nicht gegeben. Kohls Anwalt Thomas Hermes hatte schon vor dem OLG-Urteil angekündigt, den Verlag und den Autor Schwan auf Schadenersatz in Millionenhöhe verklagen zu wollen (Oberlandesgericht Köln: Bestätigung des Verbots der Nutzung von Kohl-Zitaten im Buch „Vermächtnis – die Kohl-Protokolle“, PM OLG Köln 05.05.2015; Dörries, Die Geheimnisse des Ghostwriters, SZ 13.05.2015).

LG Heilbronn

Beweisverwertungsverbot bei Dashcam-Videos

Das Landgericht (LG) Heilbronn hat mit Urteil vom 17.02.2015 entschieden, dass Aufnahmen von Dashcams im Zivilprozess regelmäßig nicht als Beweismittel zum Hergang eines Unfalls verwertet werden können (Az. I 3 S 19/14). Die Aufzeichnung von Personen mittels Dashcam stelle eine Verletzung des allgemeinen Persönlichkeitsrechts und des Rechts auf informationelle Selbstbestimmung dar, die auch nicht durch das Interesse an einer Beweissicherung gerechtfertigt sei: „Wollte man dies anders sehen und der bloßen Möglichkeit, dass eine Beweisführung erforderlich werden könnte, den Vorrang vor dem Recht auf informationelle Selbstbestimmung einräumen, würde dies bedeuten, dass innerhalb kürzester Zeit jeder Bürger Kameras ohne jeden Anlass nicht nur in seinem Pkw, sondern auch an seiner Kleidung befestigen würde, um damit zur Dokumentation und als Beweismittel zur Durchsetzung von möglichen Schadensersatzansprüchen jedermann permanent zu filmen und zu überwachen. Damit aber würde das Recht auf informationelle Selbstbestimmung praktisch aufgegeben.“

Der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, begrüßt das Urteil: „Die aktuelle Entscheidung des Landgerichts Heilbronn ist eine gute Nachricht.“ Er weist darauf hin, dass das unzulässige Filmen mit einer Dashcam mit einem hohen Bußgeld geahndet werden kann. Das für Bußgeldverfahren in Baden-Württemberg insoweit zuständige Regierungspräsidium Karlsruhe habe bereits mehrere Bußgeldverfahren wegen Dashcams eingeleitet (PE LfD Baden-Württemberg 20.02.2015, Aufnahmen von Dashcams dürfen im Zivilprozess nicht als Beweismittel zum Hergang eines Unfalls verwertet werden).

AG Frankfurt

Mieter erfolgreich gegen Video-Überwachungs-Attrappe im Hauseingang

Das Amtsgericht Frankfurt hat mit Urteil vom 29.01.2015 entschieden, dass Mieter Attrappen einer Überwachungskamera im Hauseingang und im Treppenhaus nicht akzeptieren muss (33 C 3407/14). Eine solche war von einem Vermieter zur Abschreckung von Straftätern im Hausflur angebracht worden. Er muss die Kamera jetzt wieder entfernen. Der Vermieter hatte vorgetragen, das Gerät sei nicht funktionsfähig. Deshalb werde das Persönlichkeitsrecht des Mieters auch nicht beeinträchtigt. Der Mieter klagte gegen die Attrappen, weil er sich beobachtet und eingeschüchtert fühlte. Das Gericht gab dem Mieter Recht: Schon die „mit der Anbringung der Attrappe verbundene Androhung der ständigen Überwachung“ schränke die Handlungsfreiheit des Mieters und seiner Besucher ein. Darin liege eine Verletzung des allgemeinen Persönlichkeitsrechts. Es gibt aber auch andere Entscheidungen zu diesem Thema. Das Amtsgericht Berlin-Schöneberg verneinte mit Urteil vom 30.07.2014 eine Verletzung des Persönlichkeitsrechts, wenn der Vermieter den Bewohnern mitgeteilt hat, dass die Kameras nur Attrappen sind (103 C 160/14; Mieter müssen keine Attrappe einer Video-Überwachungskamera im Hauseingang akzeptieren, www.rechtsindex.de; Angebracht, SZ, 13.02.2015, 32).



Buchbesprechungen



datACT – data protction in anti-trafficking action
Herausforderungen des Datenschutzes in der Politik gegen Menschenhandel
Ein Praxisleitfaden
Hrsg.: Bundesweiter Koordinierungskreis gegen Menschenhandel e. V. (KOK e. V.)
Berlin 2015, 112 S.

(tw) So weit und breit gestreut Datenschutzliteratur für das allgemeine Publikum und für spezifische Verwaltungs- und Wirtschaftszusammenhänge ist, so defizitär bearbeitet bleiben bisher Datenschutzthemen in Bezug auf diskriminierte Minderheiten. Die haben regelmäßig keine Ressourcen, um ihr Recht auf informationelle Selbstbestimmung wahrzunehmen und oft auch keine Fürsprecher, stecken zumeist in der Klemme zwischen privater und staatlicher Fürsorge, sozialer und hoheitlicher Repression sowie informationeller Diskriminierung; zugleich ist ihr Bedarf an Selbstbestimmung regelmäßig weit höher als bei Durchschnittsmenschen.

Einer solchen diskriminierten Minderheit hat sich der KOK angenommen, der sich auf der Basis eines Forschungsprojektes mit dem Datenschutz für vom Menschenhandel betroffenen Menschen befasst. Als ein Ergebnis dieses Projektes liegt ein Büchlein vor, das für Menschen geschrieben ist, die sich mit Menschenhandel befassen. Die Betroffenen selbst werden den Praxisleitfaden wohl realistischerweise nicht zur Hand nehmen. Umso wichtiger ist es, dass Mitarbeitende von Nichtregierungsorganisationen wie von staatlichen Hilfeeinrichtungen sich der informationellen Schutzproblematik bewusst werden und die nötigen und verfügbaren rechtlichen Instrumente kennenlernen.

Von Menschenhandel Betroffene bewegen sich regelmäßig in Gefahr privater Drangsalierung, z. B. durch kriminelle Schlepper und Zuhälter, sowie staatlicher Verfolgung durch Polizei und Ausländerbehörden. Wichtig ist deshalb einerseits eine wirksame Hilfe, andererseits die informationelle Abschottung im Schutz von größtmöglicher Anonymität. Welche rechtlichen Instrumente insofern in der EU-Datenschutzrichtlinie sowie in der Datenschutzkonvention des Europarats (Konvention 108) vorgesehen sind, ist den meisten Hilfspersonen nicht bekannt und wird plausibel dargelegt. Dabei begründen die AutorInnen, weshalb die Betroffenen von zwangsweiser Sexarbeit den besonderen rechtlichen Schutz von „sensiblen Daten“ genießen, was von Regierungsseite möglicherweise bestritten wird. Dann wird dargelegt, welche – rudimentären – Datenschutzvorkehrungen in den Rechtsinstrumenten zur Bekämpfung des Menschenhandels vorgesehen sind. Schließlich werden Tipps gegeben, wie Datenschutz in Hilfsorganisationen umgesetzt werden kann, wobei zugleich auf die vorhandenen Datenbanken, Leitlinien und Werkzeuge der (teilweise statistischen) Datenerhebung hingewiesen wird. Der Hilfebereich wird im Anhang um einen Rechtekatalog der Datensubjekte und um Datenschutzstandards ergänzt.

Das Büchlein ist allen, die in diesem Bereich tätig sind, dringend zu empfehlen. Die geleistete Arbeit müsste fortgeschrieben werden, da sich das Projekt auf den europäischen Rechtsrahmen beschränkt und die nationalen Regelungen, die teilweise das europäische und internationale Recht umsetzen, nicht behandelt. Wünschenswert wäre es, wenn im Rahmen der Umsetzung der Richtlinien weitere praktische Empfehlungen und Hilfen entwickelt und verbreitet würden. Der Verdienst der Arbeit ist, dass auf ein bisher nicht erforschtes Datenschutzproblem hingewiesen und die Grundlagen dazu erarbeitet wurden. Es ist zu wünschen, dass die hier erlangten Erkenntnisse in die Köpfe und in die Praxis der Hilfspersonen Eingang finden und so einer Gruppe von fremdbestimmten entwürdigten Menschen ein wenig Selbstbestimmung und Würde zurückgegeben wird. Die Studie ist auch im Internet verfügbar unter http://www.datact-project.org/fileadmin/user_upload/pdf/datAct_deutsch_Online.pdf.



Gola/Schomerus
BDSG Bundesdatenschutzgesetz
Kommentar
bearbeitet von Peter Gola, Christoph Klug u. Barbara Körffer, C. H. Beck, München, 12. Aufl. 2015, ISBN 978 3 406 67176 0, 677 S., 65 €

(tw) Die Kommentierung des Datenschutzrechts war, als Ordemann/Schomerus die erste Auflage ihres Kommentars herausbrachten, noch eine exotische Publikation. Inzwischen liegt die 12. Auflage vor und das Kommentieren des Daten-

schutzrechtes ist eine respektable und für Verlage lukrative Aktivität geworden. Der Gola/Schomerus ist der älteste BDSG-Kommentar, bei dem von den frühen bis zur heutigen Auflage eine personelle Kontinuität gewahrt ist. Und das erweist sich in vieler Hinsicht: So gewann der Kommentar mit jeder Auflage an Substanz und Umfang und mauserte sich immer mehr zu einer Fundgrube von Datenschutzquellen, Informationen und Materialien, die selbst für den Datenschutzspezialisten von hoher Relevanz sind – hoch komprimiert und zu einem akzeptablen Preis. Er füllt so eine Lücke zwischen den sonstigen Praktiker-Kommentaren und dem manchmal überepischen „Simitis". Man findet historische Quellen mit aktueller Relevanz ebenso wie die jüngere Literatur und Rechtsprechung. Selbst die Entwicklung unseres Datenschutzrechtes lässt sich nachvollziehen.

Diese Vorteile können aber – je nach Adressatenkreis – bei der Nutzung auch zu Problemen führen: Der quellengespickte Text setzt, wenn man ihn in der Praxis verwenden will, eine gewisse Erfahrung voraus. Das zeitliche Fortschreiben führte teilweise dazu, dass sich die Gliederung der einzelnen Paragrafen nicht sofort erschließt. Auch muss man nicht alle inhaltlichen Positionen des Kommentars teilen. Dass diese Positionen aber bestens reflektiert sind, dafür stehen die drei Bearbeitenden, die – wenn man das nicht ganz wörtlich nimmt – im besten Sinne „alte Hasen" des Datenschutzes sind, die sich nicht nur durch langjährige Tätigkeit in diesem Bereich, sondern auch durch besonderes Engagement für die Sache ausgezeichnet haben und weiter auszeichnen.

Anders als manche andere BDSG-Kommentare beschränkt sich dieser auf das BDSG und hat nicht weitere Nebengesetze im Blick. Abgedruckt sind die EG-Datenschutzrichtlinie und ein sehr brauchbares Stichwortverzeichnis. Den einzelnen Paragrafen sind spezielle Literaturangaben vorangestellt. Wer die jeweiligen Bezüge zum allgemeinen Datenschutzrecht der Länder sucht, findet diese am Ende der jeweiligen kommentierenden Texte. So bewahrt „der Gola/Schomerus" trotz der gewachsenen Konkurrenz seinen Sonderstatus und seine Relevanz bei der Auslegung des deutschen Datenschutzrechts.



Hoffmann, Christian / Luch, Anika D. / Schulz, Sönke E. / Borchers, Kim Corinna
Die digitale Dimension der Grundrechte
DIVSI-Perspektiven, Hrsg.: Deutsches Institut für Vertrauen und Sicherheit im Internet
Nomos Baden-Baden, 2015, 221 S., ISBN 978-3-8487-2027-9

(tw) Der Herausgeber, das DIVSI, hat sich offensichtlich zur Aufgabe gemacht, die rechtlichen und gesellschaftlichen Grundlagen der Digitalisierung unserer Informationsgesellschaft zu dokumentieren. Mit dem vorliegenden Werk wird durch das Lorenz-von-Stein-Institut in Kiel die digitale Dimension der Grundrechte bearbeitet. Im Vorwort konstatiert der frühere Präsident des Bundesverfassungsgerichts und frühere Bundespräsident Roman Herzog richtig, dass die klassischen wissenschaftlichen Grundrechtskommentierungen die digitale Dimension der Verfassung noch nicht hinreichend würdigten. Am Ende des Buches konstatieren die Autoren auch zutreffend, dass die Gerichte insofern Vorreiter sind. Tatsächlich hinkt nicht nur die Politik, sondern auch die Rechtswissenschaft hinterher. Dass sie sich hierbei bemüht, zeigt der vorliegende Band, der dabei auf Einzelaufsätze, auf einige ausführlichere Werke und insbesondere auf die Rechtsprechung, die dem prallen digitalen Leben entspringt, zurückgreift.

Das Anliegen des Buches ist es, zur Behebung des bestehenden Defizits, die Grundrechte des Grundgesetzes auf digitale Anwendungsfälle abzuklopfen: von der Menschenwürde über die allgemeine Handlungsfreiheit, natürlich über die vielfältigen Facetten des allgemeinen Persönlichkeitsrechts bis hin zu eher analog erscheinenden Grundrechten: körperliche Unversehrtheit, Film- und Kunstfreiheit, Schutz von Wohnung, Familie, Beruf, Religion, Schule, Versammlung, Vereinigung, Freizügigkeit, Beruf, Eigentum. Natürlich bearbeitet sind auch die Informations- und Kommunikationsgrundrechte: Schutz von Meinung, Presse, Rundfunk, Fernmeldegeheimnis und Petition. Herausgekommen ist eine sehr konzentrierte und valide Ansammlung von praktischen Fällen mit Grundrechtsrelevanz, mit denen wir in der jüngeren Vergangenheit konfrontiert wurden.

Das Buch ist gut informiert und materialreich und insofern eine Fundgrube. Wie dem Ausblickkapitel zu entnehmen ist, war es nicht der Anspruch an die AutorInnen, eine Theorie oder eine Struktur der digitalen Grundrechte zu entwickeln. Ansätze dazu finden sich – systematisch etwas überraschend – bei den Ausführungen zu Art. 11 GG, also zur Freizügigkeit, wo die Grundrechtsrelevanz von gegenständlichen und digitalen Räumen einander gegenübergestellt wird. Im Ausblick wird zudem ausgeführt, dass der digitale Grundrechtsschutz insbesondere Infrastrukturschutz bedingt. Hier wäre es spannend gewesen, was dies für staatliche Infrastrukturangebote und technische Möglichkeiten des Selbstschutzes, etwa durch Nutzung von Kryptografie, bedeutet.

Das Internet wird geprägt von folgenden Merkmalen: Virtualität, Konvergenz, Globalität und Intransparenz. Jedes diese Merkmale hat Grundrechtsrelevanz, doch behandelt werden in dem Buch nur die ersten beiden. Welche Auswirkungen die Globalität mit weltweit unterschiedlichen Grundrechtsstandards hat, muss an anderer Stelle bearbeitet werden, ebenso die Frage, wie durch Transparenz der digitalen Datenverarbeitung Grundrechte gesichert werden können.

Dies führt uns erneut zur Infrastrukturverantwortung des Staates. Angesichts der rasanten technischen Entwicklung darf und kann sich diese nicht auf die Fortschreibung der

analogen Grundrechte beschränken, sondern wird vor strukturelle Herausforderungen gestellt: Eine dieser Herausforderungen ist in der juristische Debatte noch nicht angekommen, wohl aber im Feuilleton besserer Zeitungen: die grundrechtsbeschränkende Kraft von auf Computeranalyse à la Big Data basierenden Entscheidungen. Hierzu hat Lawrence Lessig in seinem Essay „Code is law" schon vor 15 Jahren eindringlich die freiheitsgefährdenden Wirkungen der Digitalisierung beschrieben. Die Notwendigkeit der Entwicklung einer „vierten" unabhängigen Gewalt zur Vertretung der digitalen Grundrechtsinteressen, die ansonsten keine Lobby finden. Hier bieten sich die Datenschutz- und Informationsfreiheitsbeauftragten an. Die aktuell wohl gravierendste Strukturherausforderung sind die privaten Monopole, welche die Frage der Drittwirkung von Grundrechten und kompensierender staatlicher Garantien aufwirft. Das vorliegende Buch liefert insofern Anwendungsbeispiele, aber keine Analyse und keine Lösungen. Weniger als das: Wieder kann es sich das von DIVSI herausgegebene Werk des Lorenz-von-Stein-Instituts nicht verkneifen, das Verbot mit Erlaubnisvorbehalt im Datenschutzbereich in Frage zu stellen (S. 52). Auch mit der Behauptung, die Überbetonung des Zweckbindungsgrundsatzes berge angesichts neuartiger Analysemöglichkeiten (Big Data) „die Gefahr, innovationshemmend zu wirken" (S. 36), verbleibt das Buch im Deskriptiven und bedient ein Vorurteil, mit dem die Politik regelmäßig ihre mangelnde Innovationsbereitschaft im digitalen Grundrechtsbereich begründet.

Das Verdienst des Buches ist es, Material zum digitalen Grundrechtsschutz zu liefern und aufzubereiten. Es macht die eingangs von Herzog kritisierte Digitalabstinenz der Juristerei an die modernen Zeiten anschlussfähig. Bezugspunkt bleibt dabei das Grundgesetz. Inzwischen haben wir die Europäische Grundrechte-Charta, die mit ihrem Inkrafttreten 2009 nicht nur zeitlich näher an der Digitalisierung ist als das Grundgesetz des Jahres 1949. Diesem Mosaikstein in der digitalen Grundrechtspräsentation müssen weitere folgen.



Kingreen, Thorsten / Kühling, Jürgen (Hrsg.)
Gesundheitsdatenschutzrecht
Nomos Baden-Baden, 2015, 490 S., ISDN 978-3-8487-1680-7

(tw) Der Titel ist so kurz wie aussagekräftig. Zum Gesundheitsdatenschutzrecht gibt es Tausende Artikel und Studien. Aber auch nach 45 Jahren Datenschutzrecht hatte es bisher noch niemand geschafft, eine umfassende und inhaltlich einigermaßen befriedigende Darstellung des Gesundheitsdatenschutzrechtes abzuliefern. Mit diesem Werk ist dies, als Ergebnis eines von der Deutschen Forschungsgemeinschaft geförderten Gemeinschaftsprojektes, weitgehend gelungen. Der Grund für die lange literarische Durststrecke ist der zentrale Inhalt dieses dicken Buches: Das Gesundheitsdatenschutzrecht ist derart verworren und unübersichtlich und teilweise nur situativ zu erklären, dass selbst SpezialistInnen nur ansatzweise einen Gesamtüberblick haben. Selbst bei umfassender Kenntnis sämtlicher anzuwendenden Rechtsnormen geben diese keine problemadäquaten Antworten auf die früheren und schon gar nicht auf die aktuellen Herausforderungen des eHealth für die patientenbezogene Datenverarbeitung: BDSG, LDSG, kirchliches DSR, SGB V, SGB X, SGB I, Ärztliche und andere heilberufliche Berufsordnungen, Gendiagnostikgesetz, Landeskrankenhausgesetze… Doch auch diesmal hat es mit der umfassenden Darstellung nicht ganz geklappt: Die bereichsspezifischen Datenschutzregelungen werden nur exemplarisch an zwei Beispielen erwähnt, einem Krankenhausgesetz und dem Arzneimittelgesetz. Aber die bereichsspezifischen Regeln sind nicht das Hauptproblem, unübersichtlich sind schon und insbesondere die allgemeinen Regelungen im Dreiecksverhältnis von PatientInnen, Leistungserbringern und Leistungsträgern – jeweils mit deren Dienstleistern.

Dargestellt werden zunächst die allgemeinen datenschutzrechtlichen Grundlagen, wozu es schon mehr als genug Literatur gibt. Auf diesen schon sehr umfangreichen Teil hätten die AutorInnen weitgehend verzichten können. Dann aber werden in weiteren Einzelkapiteln die wichtigsten spezifischen Anwendungsfelder dargestellt: Gesundheitswesen inclusive GKV- und privatärztlicher Abrechnung, Familie, medizinische Forschung, private Versicherungsverträge, Arbeitsleben.

Ein Zweck des Projektes war es, einen Überblick zu schaffen und die wesentlichsten regulatorischen Defizite zu benennen. Dies gelingt den AutorInnen. Sie beschreiben, wie sich selbst die Richter des Bundessozialgerichtes 2008 bei der privaten Beauftragung im Rahmen der GKV-Abrechnung im rechtlichen Gestrüpp verirrten, als sie einwilligungsbasierte Lösungen verwarfen.

Bei allem Lob für das Werk muss von einem Praktiker, der seit über 30 Jahren Gesundheitsdatenschutz anwendet, darauf hingewiesen werden, dass auch dieses Werk selbst in den medizinischen Kernbereichen keinen vollständigen Überblick über das Wesentliche liefert. Zwei Beispiele: Den aus der Wissenschaft kommenden AutorInnen scheint entgangen zu sein, dass die Datenschutzaufsichtsbehörden mit der Versicherungswirtschaft ein Einwilligungsverfahren zur Schweigepflichtentbindung abgesprochen haben, das den Anforderungen des Bundesverfassungsgerichtes in dieser Frage gerecht zu werden versucht. Auch die praktischen Probleme beim Einsatz von IT-Dienstleistern werden nicht adäquat gewürdigt. Ein Defizit des Buchs besteht darin, dass es sich auf die rechtsdogmatische Darstellung beschränkt und die technischen Rahmenbedingungen allenfalls am Rande behandelt.

Wünschenswert wäre auch gewesen, wenn die rechtlichen Normen nicht nur dargestellt, sondern auch detaillierter in ihrer lebenspraktischen Bedeutung erläutert würden. Beides scheint aber nicht Gegenstand des Forschungsprojektes gewesen zu sein, auf dem das Buch basiert.

Ein Grund, weshalb es bisher keine Gesamtdarstellung gab, könnte auch sein, dass es zu wenige Adressaten für eine derartige wissenschaftlich seriöse Darstellung gibt. Die MedizinrechtlerInnen betreiben Datenschutz zumeist nur als Beifang. Für viele DatenschutzrechtlerInnen ist das Sujet zu kompliziert, für medizinische Leistungserbringer, IT-lerInnen und PatientInnen ohnehin; die Politik hat sich um das Regelungschaos bisher nicht gekümmert. Das könnte sich ändern, auch nun dank der vorliegenden Studie. Zwar gibt diese keine genauen Tipps, wie aus der Diagnose eine Therapie möglich wäre. Angesichts aber die Umstandes, dass die Europäische Datenschutzgrundverordnung Anlass sein müsste, das gesamte nationale Datenschutzrecht auch in solchen Spezialgebieten neu aufzusetzen, kann dank der nun vorliegenden Übersicht das Wesentliche vom Unwesentlichen getrennt werden. Ganz offensichtlich ist, dass der Versuch einer konsistenten Vollregelung in den Sozialgesetzbüchern misslungen ist. Es ist aber weiterhin fraglich, ob der Bundesgesetzgeber bereit sein wird, diesen Augias-Stall auszumisten. Schade ist, dass das Buch kein Stichwortverzeichnis aufweist, was das Auffinden relevanter Aussagen erleichtern würde.



Monika Kuschewsky (Hrsg.)
Data Protection & Privacy,
2nd Edition
Thomson Reuters, London, 2014
ISBN 9780414032521
200 GBP

(ks) Dieses Werk ist ein verborgener Schatz. Verborgen, weil es in Deutschland bisher wenig bekannt und schwer erhältlich ist. Selbst der Online-Buchhändler, der sonst fast alles beschafft, führt es nicht im Sortiment. Ein Schatz nicht nur, weil es einen selbst für juristische Werke stolzen Betrag hinzublättern gilt.

Als Datenschützer mit internationalen Kunden, Betriebsstätten, Konzernen kennt man die Situation: Plötzlich findet ein Teil einer Datenverarbeitung in einem Land außerhalb Deutschlands, möglicherweise gar außerhalb der EU statt – und die dortige Datenschutzlage ist einem völlig unbekannt. Es folgt meist eine mehr oder weniger erfolgreiche Recherchephase im Internet, die einem zumindest ein bisschen Klarheit über das Rechtssystem, die Bezeichnung evtl. bestehender Datenschutzgesetze und die wichtigsten Datenschutz-Rahmenbedingungen verschaffen soll. Wer immer diese Situation kennt, weiß auch, wie zeitraubend und frustrierend die Suche nach Überblick sein kann – obwohl man doch meinen könnte, dass im Zeitalter des Internets derartige Informationen auf Fingerschnipp zur Verfügung stünden.

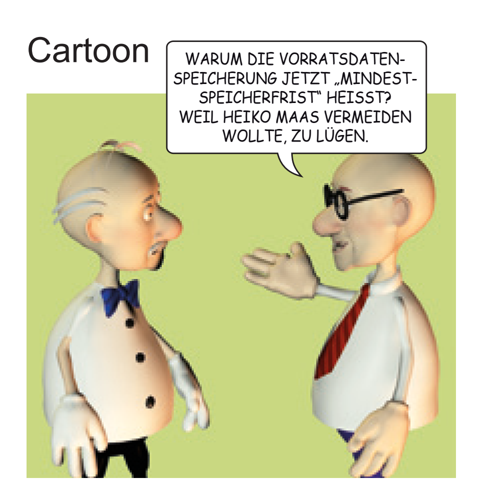
Dass zumindest für 36 Staaten und 3 Großregionen der Überblick über die Datenschutzgesetzgebung sehr leicht zu gewinnen ist, ist der Verdienst von Monika Kuschewsky und ihren Ko-Autoren. Aufnahme in das Werk fanden Länder, die eine nennenswerte Datenschutzgesetzgebung vorweisen können. Dass darunter wirtschaftlich besonders stark mit Europa verflochtene Nationen zu finden sind, steigert den Nutzen für Praktiker. Neben vielen europäischen Ländern findet man Israel, Australien, Japan und natürlich die USA. Aber auch Indien, Malaysia, Mexiko, Brasilien oder die Türkei. Etwas schade, dass Russland keine Aufnahme gefunden hat.

Um den Überblick zu erleichtern und eine schnelle Vergleichbarkeit zu ermöglichen, folgen alle Autoren einem äußerst übersichtlichen Schema. Systematisch werden für jedes Land die wesentlichen Aspekte der Datenschutzlage unter den gleichen Hauptüberschriften dargestellt: Gesetzgebung, Datenschutzbehörden, Zulässigkeitsgrundlagen, Spezialgesetzgebung, Qualitätsanforderungen, Outsourcing, Internationaler Datenverkehr, Informationspflichten, Betroffenenrechte, Sicherheitsanforderungen, Technikfolgenabschätzung und Audits, Meldepflichten, Datenschutzbeauftragter, Umsetzungsverfolgung, Rechtsmittel und Haftung.

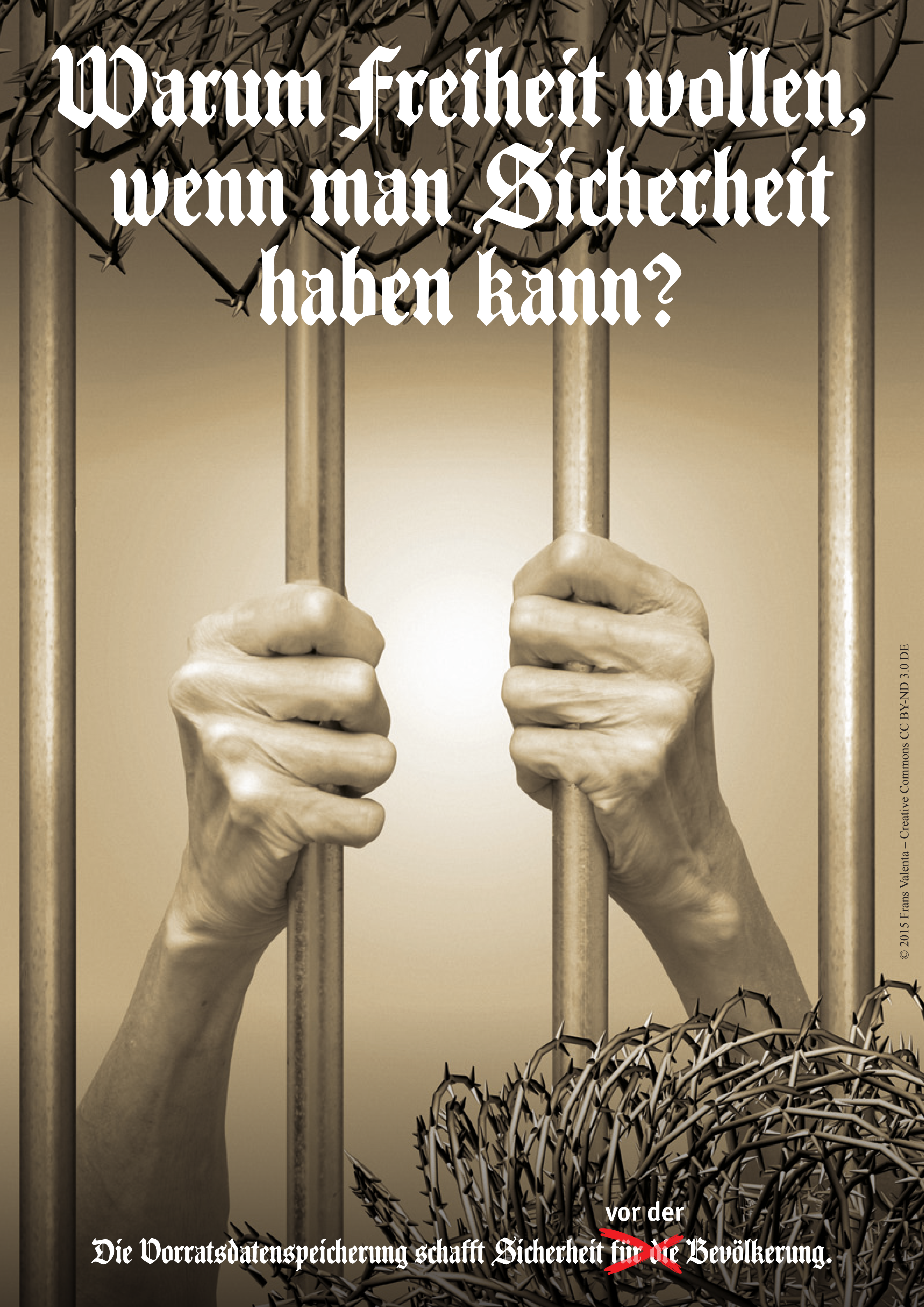
So lassen sich alle wesentlichen Aspekte der Datenschutzlage in einem Land schnell erfassen und bieten eine gute Grundlage für weiteres, vertiefendes Studium, falls erforderlich.

Das Werk stellt damit für Datenschutzbeauftragte, IT-Sicherheitsbeauftragte, Compliance Officer, Konzernbetriebsräte und sonstige, mit internationalem Datenverkehr konfrontierte Personengruppen eine in höchstem Maße wertvolle Quelle strukturierter Erstinformation dar. Ihm wäre eine kontinuierliche Erweiterung um zusätzliche Länderdarstellungen und, zum Nutzen für weitere Lesergruppen, eine Übersetzung ins Deutsche zu wünschen.

Cartoon






Warum Freiheit wollen, wenn man Sicherheit haben kann?
vor der
Die Vorratsdatenspeicherung schafft Sicherheit ~~für die~~ Bevölkerung.
© 2015 Frans Valenta – Creative Commons CC BY-ND 3.0 DE